Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019119

International filing date: 21 December 2004 (21.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-001359
Filing date: 06 January 2004 (06.01.2004)

Date of receipt at the International Bureau: 17 February 2005 (17.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP2004/019119

22.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　１月　６日

出願番号
Application Number: 特願２００４－００１３５９

[ST. 10/C]: [ＪＰ２００４－００１３５９]

出願人
Applicant(s): ソニー株式会社

２００５年　２月　４日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３００６８２

【書類名】　特許願
【整理番号】　0390873002
【提出日】　平成16年 1月 6日
【あて先】　特許庁長官殿
【国際特許分類】　G06K 17/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　栗田　太郎
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100093241
　【弁理士】
　【氏名又は名称】　宮田　正昭
【選任した代理人】
　【識別番号】　100101801
　【弁理士】
　【氏名又は名称】　山田　英治
【選任した代理人】
　【識別番号】　100086531
　【弁理士】
　【氏名又は名称】　澤田　俊夫
【手数料の表示】
　【予納台帳番号】　048747
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9904833

【書類名】特許請求の範囲
【請求項１】
メモリ空間を備え、１以上のファイル・システムに分割して管理するデータ通信装置であって、
外部機器又はプログラムからのアクセスに対し、ファイル・システム毎に相互認証又は暗証コードの照合手続きを要求する認証手段と、
アクセスに対し、相互認証又は暗証コードの照合手続きが要求されている認証状態、又は相互認証手続き又は暗証コードの照合手続きを経てアクセスが許可されている解除状態のいずれであるかをファイル・システム毎に管理する認証情報管理手段と、
所定の事象の発生に応じてファイル・システムの解除状態を認証状態に戻す状態管理手段と、
を具備することを特徴とするデータ通信装置。
【請求項２】
前記状態管理手段は、外部機器又はプログラムがアクセス先のファイル・システムを変更したとき、元のアクセス先のファイル・システムの解除状態を認証状態にリセットする、
ことを特徴とする請求項１に記載のデータ通信装置。
【請求項３】
前記状態管理手段は、ファイル・システムが解除状態となってから所定期間が経過した後、あるいは電源投入後所定時間経過した後に認証状態にリセットする、
ことを特徴とする請求項１に記載のデータ通信装置。
【請求項４】
メモリ空間を備え、１以上のファイル・システムに分割して管理するデータ通信装置のメモリ管理方法であって、
外部機器又はプログラムからのアクセスに対し、ファイル・システム毎に相互認証又は暗証コードの照合手続きを要求する認証ステップと、
アクセスに対し、相互認証又は暗証コードの照合手続きが要求されている認証状態、又は相互認証手続き又は暗証コードの照合手続きを経てアクセスが許可されている解除状態のいずれであるかをファイル・システム毎に管理する認証情報管理ステップと、
所定の事象の発生に応じてファイル・システムの解除状態を認証状態に戻す状態管理ステップと、
を具備することを特徴とするデータ通信装置のメモリ管理方法。
【請求項５】
前記状態管理ステップでは、外部機器又はプログラムがアクセス先のファイル・システムを変更したとき、元のアクセス先のファイル・システムの解除状態を認証状態にリセットする、
ことを特徴とする請求項４に記載のデータ通信装置のメモリ管理方法。
【請求項６】
前記状態管理ステップでは、ファイル・システムが解除状態となってから所定期間が経過した後、あるいは電源投入後所定時間経過した後に認証状態にリセットする、
ことを特徴とする請求項４に記載のデータ通信装置のメモリ管理方法。

【書類名】明細書
【発明の名称】データ通信装置及びデータ通信装置のメモリ管理方法
【技術分野】
【０００１】
本発明は、比較的大容量のメモリ領域を備えたデータ通信装置及びデータ通信装置のメモリ管理方法に係り、特に、メモリ領域上に電子的な価値情報を格納して電子決済を始めとするセキュアな情報のやり取りを行なうデータ通信装置及びデータ通信装置のメモリ管理方法に関する。
【０００２】
さらに詳しくは、本発明は、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供するデータ通信装置及びデータ通信装置のメモリ管理方法に係り、特に、外部機器との間のセッションをファイル・システム毎に管理し、ファイル・システム毎に独立してセキュリティに関する脅威を分析、管理、並びに運用するデータ通信装置及びデータ通信装置のメモリ管理方法に関する。
【背景技術】
【０００３】
局所でのみ適用可能な無線通信手段の一例として、非接触ＩＣカードを挙げることができる。
【０００４】
この種の無線通信には、一般に、電磁誘導の原理に基づいて実現される。すなわち、メモリ機能を有するＩＣカードと、ＩＣカードのメモリに対して読み書きアクセスをするカード・リーダ／ライタで構成され、１次コイルとしてのＩＣカード側のループ・コイルと２次コイルとしてのカード・リーダ／ライタ側のアンテナが系として１個のトランスを形成している。そして、カード・リーダ／ライタ側からＩＣカードに対して、電力と情報を同じく電磁誘導作用により伝送し、ＩＣカード側では供給された電力によって駆動してカード・リーダ／ライタ側からの質問信号に対して応答することができる。
【０００５】
カード・リーダ／ライタ側では、アンテナに流す電流を変調することで、ＩＣカード上のループ・コイルの誘起電圧が変調を受けるという作用により、カード・リーダ／ライタからＩＣカードへのデータ送信を行なうことができる。また、ＩＣカードは、ループ・コイルの端子間の負荷変動により、ＩＣカード・リーダ／ライタ側のアンテナ端子間のインピーダンスが変化してアンテナの通過電流や電圧が変動するという作用により、カード・リーダ／ライタへの返信を行なう。
【０００６】
ＩＣカードに代表される非接触・近接通信システムは、操作上の手軽さから、広範に普及している。例えば、暗証コードやその他の個人認証情報、電子チケットなどの価値情報などをＩＣカードに格納しておく一方、キャッシュ・ディスペンサやコンサート会場の出入口、駅の改札口などにカード・リーダ／ライタを設置しておく。そして、利用者がＩＣカードをカード・リーダ／ライタにかざすことで、非接触でアクセスし、認証処理を行なうことができる。
【０００７】
最近では、微細化技術の向上とも相俟って、比較的大容量のメモリ空間を持つＩＣカードが出現している。大容量メモリ付きのＩＣカードによれば、複数のアプリケーションを同時に格納しておくことができるので、１枚のＩＣカードを複数の用途に利用することができる。例えば、１枚のＩＣカード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケットなど、多数のアプリケーションを格納しておくことにより、１枚のＩＣカードをさまざまな用途に適用させることができる。ここで言う電子マネーや電子チケットは、利用者が提供する資金に応じて発行される電子データを通じて決済（電子決済）される仕組み、又はこのような電子データ自体を指す。

【０００８】
ＩＣカードの一般的な使用方法は、利用者がＩＣカードをカード・リーダ／ライタをかざすことによって行なわれる。カード・リーダ／ライタ側では常にＩＣカードをポーリングしており外部のＩＣカードを発見することにより、両者間の通信動作が開始する。
【０００９】
このとき、利用者が暗証番号をＩＣカード・リーダ側に入力して、入力された暗証番号をＩＣカード上に格納された暗証番号と照合することで、ＩＣカードとＩＣカード・リーダ／ライタ間で本人確認又は認証処理が行なわれる。（ＩＣカード・アクセス時に使用する暗証番号のことを、特にＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）と呼ぶ。）そして、本人確認又は認証処理に成功した場合には、例えば、ＩＣカード内に保存されているアプリケーションの利用、すなわち、アプリケーションに割り当てられているサービス・メモリ領域へのアクセスが可能となる（本明細書中では、アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ）。サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。
【００１０】
さらに、ＩＣカードやカード用リーダ／ライタ（カード読み書き装置）が無線・非接触インターフェースの他に、外部機器と接続するための有線インターフェース（図示しない）を備えることにより、ＩＣカードやリーダ／ライタの機能を携帯電話機、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｃｅ）やパーソナル・コンピュータなどの各デバイスにＩＣカード及びカード・リーダ／ライタのいずれか一方又は双方の機能を装備することができる。このような場合、ＩＣカード技術を汎用性のある双方向の近接通信インターフェースとして利用することができる。
【００１１】
例えば、コンピュータや情報家電機器のような機器同士で近接通信システムが構成される場合には、ＩＣカードによる非接触通信通信は一対一で行なわれる。また、ある機器が非接触ＩＣカードのような機器以外の相手デバイスと通信することも可能であり、この場合においては、１つの機器と複数のカードにおける一対多の通信を行なうアプリケーションも考えられる。
【００１２】
また、電子決済を始めとする外部との電子的な価値情報のやり取りなど、ＩＣカードを利用したさまざまなアプリケーションを、情報処理端末上で実行することができる。例えば、情報処理端末上のキーボードやディスプレイなどのユーザ・インターフェースを用いてＩＣカードに対するユーザ・インタラクションを情報処理端末上で行なうことができる。また、ＩＣカードが携帯電話機と接続されていることにより、ＩＣカード内に記憶された内容を電話網経由でやり取りすることもできる。さらに、携帯電話機からインターネット接続して利用代金をＩＣカードで支払うことができる。
【００１３】
このように、あるサービス提供元事業者用のファイル・システムをＩＣカードの内蔵メモリに割り当てて、このファイル・システム内で当該事業者によるサービス運用のための情報（例えば、ユーザの識別・認証情報や残りの価値情報、使用履歴（ログ）など）を管理することにより、従来のプリペイド・カードや店舗毎のサービス・カードに置き換わる、非接触・近接通信を基調とした有用なサービスを実現することができる。
【００１４】
従来、サービス提供元事業者毎にＩＣカードが個別に発行され、ユーザの利用に供されていた。このため、ユーザは、享受するサービス毎にＩＣカードを取り揃え、携帯しなければならなかった。これに対し、比較的大容量のメモリ空間を持つＩＣカードによれば、単一のＩＣカードの内蔵メモリに複数のサービスに関する情報を記録するだけの十分な容量を確保することができる。
【００１５】

ここで、プリペイド・カードなどの前払式証票に関しては、その発行などの業務の適正な運営を確保して、前払式証票の購入者らの利益保護と前払式証票の信用維持を図ることを主な目的として、前払式証票の発行者に対して登録やその他の必要な規制を行うための「前払式証票の規制等に関する法律」（通称、「プリカ法」）が制定されており、利用者の便宜や流通秩序維持などの目的で、ロゴや問い合わせ先などの所定事項をプリペイド・カード上（券面）に表示することが義務付けられている（同法第１２条を参照のこと）。

【００１６】

ＩＣカードのメモリ機能に前払情報を格納することによってプリペイド・カードを実現する場合、法で規制される必要な情報を媒体上に印刷しておくことにより、単一のサービスしか提供できなくなる。これに対し、ＩＣカード機能を携帯電話機のような表示機能を持つ携帯端末上で利用する場合には、希望する価値情報に関連する情報を画面表示させることにより（例えば、特許文献１を参照のこと）、上記の法規制を満たすことができ、複数のサービス提供元事業者による共有が可能となる。したがって、サービス提供元事業者においてはカード発行の負担が軽減するとともに、ユーザにとっては携帯して管理するＩＣカードの枚数を削減することができる。

【００１７】

ところが、複数のサービス提供元事業者間で単一のメモリ領域を共有した場合、あるサービス提供元事業者が使用するメモリ領域を、メモリを共用する別の事業者から自由にアクセスできるようにすると、事業者毎に設定される価値情報が他の事業者によって不正利用を許してしまうことになりかねない。この結果、事業者側では健全なサービス提供を行なえなくなり、ユーザにとっては換金性の高い価値情報が流出の危機にさらされ、経済的な損害を被る。

【００１８】

したがって、ＩＣカードを複数のサービス提供元事業者間で共用する場合には、ユーザにとっては各サービス利用時において事業者自らが発行したＩＣカードであるかのような使い勝手を確保する一方、メモリ領域上の事業者毎の情報をセキュアに管理する機構を備えている必要がある。

【００１９】

【特許文献１】特開２００３－１４１４３４号公報

【発明の開示】

【発明が解決しようとする課題】

【００２０】

本発明の目的は、メモリ領域上に電子的な価値情報を格納して電子決済を始めとするセキュアな情報のやり取りを好適に行なうことができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することにある。

【００２１】

本発明のさらなる目的は、ユーザにとっては各サービス利用時において事業者自らが発行したＩＣカードであるかのような使い勝手を確保する一方、メモリ領域上の事業者毎の情報をセキュアに管理する機構を備え、単一のＩＣカードを複数のサービス提供元事業者間で共用することができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することにある。

【００２２】

本発明のさらなる目的は、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有した際に、外部機器との間のセッションをファイル・システム毎に管理し、ファイル・システム毎に独立してセキュリティに関する脅威を分析、管理、並びに運用することができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することにある。

【課題を解決するための手段】

【００２３】

本発明は、上記課題を参酌してなされたものであり、メモリ空間を備え、１以上のファ

イル・システムに分割して管理するデータ通信装置であって、
外部機器又はプログラムからのアクセスに対し、ファイル・システム毎に相互認証又は暗証コードの照合手続きを要求する認証手段と、
アクセスに対し、相互認証又は暗証コードの照合手続きが要求されている認証状態、又は相互認証手続き又は暗証コードの照合手続きを経てアクセスが許可されている解除状態のいずれであるかをファイル・システム毎に管理する認証情報管理手段と、
所定の事象の発生に応じてファイル・システムの解除状態を認証状態に戻す状態管理手段と、
を具備することを特徴とするデータ通信装置である。ここで言うデータ通信装置は、無線通信部および、データ送受信機能とデータ処理部を有するＩＣチップを内蔵する非接触ＩＣカード、表面に端子を有する接触ＩＣカード、接触／非接触ＩＣカードと同様の機能を有するＩＣチップを携帯電話機、ＰＨＳ（Ｐｅｒｓｏｎａｌ Ｈａｎｄｙｐｈｏｎｅ Ｓｙｓｔｅｍ）、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｃｅ）などの情報通信端末装置に内蔵した装置である。このデータ通信装置は、ＥＥＰＲＯＭなどのデータ蓄積メモリを含むメモリ領域とデータ処理部を有するとともに、データ通信機能を有するものである。携帯電話機などの場合は、ＩＣチップを内蔵するＩＣカードなどの外部記憶媒体を着脱可能に構成してもよい。また、携帯電話会社が発行する契約者情報を記録したＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）機能をＩＣチップに搭載してもよい。データ通信装置は、インターネット等の情報通信ネットワークを介してデータ通信を行なっても、外部端末装置と有線あるいは無線で直接データ通信を行なってもよい。

【００２４】
本発明は、ＩＣカードが持つ耐タンパ性と認証機能を利用して、価値情報のやり取りなどを含んだセキュリティが要求されるサービスを提供するものである。より具体的には、ＩＣカード内の単一のメモリ領域を複数のサービス提供元事業者間で共有し、サービス提供元事業者においてはカード発行の負担が軽減するとともに、ユーザにとっては携帯して管理するＩＣカードの枚数を削減するものである。

【００２５】
複数のサービス提供元事業者間で単一のメモリ領域を共有した場合、あるサービス提供元事業者が使用するメモリ領域を、メモリを共用する別の事業者から自由にアクセスできるようにすると、事業者毎に設定される価値情報が他の事業者によって不正利用を許してしまう、という問題がある。

【００２６】
これに対し、本発明では、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供するようにした。メモリ領域をファイル・システムに分割することにより、ファイル・システム間の境界がファイヤ・ウォールとして機能し、他のファイル・システム（すなわち他のサービス提供元事業者）からのアクセス（不正侵入）を好適に排除することができる。

【００２７】
ＩＣカード内のメモリ領域は、初期状態では、元のＩＣカード発行者がメモリ領域全体を管理している。ＩＣカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割するに際しては、メモリ領域の分割権限と、元のＩＣカード発行者に対する認証の双方を要求するようになっている。

【００２８】
このような分割操作を繰り返すことにより、ＩＣカード内のメモリ領域は複数のファイル・システムが共存する構造となる。ファイル・システムの分割は、仮想的なＩＣカードの発行である。

【００２９】
一旦分割されると、ファイル・システムへのアクセスは、元のＩＣカードの発行者では

なく、ファイル・システム自体のサービス提供元事業者への認証が要求される。すなわち、ファイル・システムへアクセスするときには、当該ファイル・システムの発行者鍵を用いた相互認証が課される。さらに秘密保持の強度などの状況に応じて、ファイル・システム又はファイル・システム内のディレクトリやファイル毎に暗証コードすなわちＰＩＮを割り当て、サービス実行時にＰＩＮの照合処理を行なうようにすることもできる。

【００３０】

ここで、ＩＣカードのメモリ領域がサービス提供元事業者毎の複数のファイル・システムに分割され、共用されるシステムにおいては、あるファイル・システムへのアクセスを試み、相互認証処理並びにＰＩＮ照合処理を経て、解除状態となりセッションが確立した際、この解除状態における他のファイル・システムのセキュリティへの影響が問題となる。何故ならば、セッションの状態が保たれると、その間、他のファイル・システムへのクラッキングの脅威があるからである。

【００３１】

そこで、本発明では、ＩＣカードのメモリ領域に複数のファイル・システムを分割する機能と、各ファイル・システム上のディレクトリやファイルに対する暗証コードの照合機能を連携させることにより、ファイル・システム毎に独立してセキュリティに関する脅威を分析、管理、並びに運用するようにした。

【００３２】

すなわち、ＩＣカードのメモリ領域上に、論理的に複数のファイル・システムが配置されている状態で、外部機器又はプログラムがアクセス先のファイル・システムを変更したとき、各メモリ領域が保持しているシステム管理情報　（相互認証情報を含む）やＰＩＮの解除情報などをリセットする。さらに、ＩＣカードへの電源投入後、一定時間（例えば、利用時期のクラッキング技術やコンピュータの処理速度から、利用しているセッション暗号スキームを絶対に解読することができない時間）が経過した後、電源をリセットすることで、同様の相互認証・ＰＩＮ照合情報をリセットする。

【００３３】

このように、システムが認証状態と解除状態を適宜切り替えることにより、セッションの状態が保たれることによるクラッキングの脅威を排除することができる。

【発明の効果】

【００３４】

本発明によれば、メモリ領域上に電子的な価値情報を格納して電子決済を始めとするセキュアな情報のやり取りを好適に行なうことができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することができる。

【００３５】

また、本発明によれば、ユーザにとっては各サービス利用時において事業者自らが発行したＩＣカードであるかのような使い勝手を確保する一方、メモリ領域上の事業者毎の情報をセキュアに管理する機構を備え、単一のＩＣカードを複数のサービス提供元事業者間で共用することができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することができる。

【００３６】

また、本発明によれば、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有した際に、外部機器との間のセッションをファイル・システム毎に管理し、各ファイル・システムのセキュリティに関する脅威を分析、管理、並びに運用することができる、優れたデータ通信装置及びデータ通信装置のメモリ管理方法を提供することができる。

【００３７】

本発明によれば、ＩＣカードのメモリ領域に複数のファイル・システムを分割する機能と、各ファイル・システム上のディレクトリやファイルに対する暗証コードの照合機能を連携させることにより、ファイル・システム毎に独立してセキュリティに関する脅威を分析、管理、並びに運用することができる。

【００３８】
本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。
【発明を実施するための最良の形態】
【００３９】
以下、図面を参照しながら本発明の実施形態について詳解する。
【００４０】
本発明は、ＩＣカードが持つ耐タンパ性と認証機能を利用して、価値情報のやり取りなどを含んだセキュリティが要求されるサービスを提供するものであり、より具体的には、ＩＣカード内の単一のメモリ領域を複数のサービス提供元事業者間で共有し、サービス提供元事業者においてはカード発行の負担が軽減するとともに、ユーザにとっては携帯して管理するＩＣカードの枚数を削減するものである。
【００４１】
ここで、複数のサービス提供元事業者間で単一のメモリ領域を共有した場合、あるサービス提供元事業者が使用するメモリ領域を、メモリを共用する別の事業者から自由にアクセスできるようにすると、事業者毎に設定される価値情報が他の事業者によって不正利用を許してしまう、という問題がある。
【００４２】
本発明では、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供するようにした。メモリ領域をファイル・システムに分割することにより、ファイル・システム間の境界がファイヤ・ウォールとして機能し、他のファイル・システム（すなわち他のサービス提供元事業者）からのアクセス（不正侵入）を好適に排除することができる。
【００４３】
ＩＣカード内のメモリ領域は、初期状態では、元のＩＣカード発行者がメモリ領域全体を管理している。ＩＣカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割するに際しては、メモリ領域の分割権限と、元のＩＣカード発行者に対する認証の双方が要求される。
【００４４】
そして、一旦分割されると、ファイル・システムへのアクセスは、元のＩＣカードの発行者ではなく、ファイル・システム自体のサービス提供元事業者への認証が要求される。したがって、ユーザにとっては、各サービス利用時において事業者自らが発行したＩＣカードであるかのような使い勝手を確保することができる。
【００４５】
さらに、ＩＣカードのメモリ領域に複数のファイル・システムを分割する機能と、各ファイル・システム上のディレクトリやファイルに対する暗証コードの照合機能を連携させることにより、ファイル・システム毎に独立してセキュリティに関する脅威を分析、管理、並びに運用することができる。
【００４６】
ここで、まず、ＩＣカード及びカード読み書き装置間の非接触データ通信の仕組みについて、図１及び図２を参照しながら説明する。
【００４７】
カード読み書き装置とＩＣカード間の無線通信は、例えば電磁誘導の原理に基づいて実現される。図１には、電磁誘導に基づくカード読み書き装置とＩＣカードとの無線通信の仕組みを概念的に図解している。カード読み書き装置は、ループ・コイルで構成されたアンテナL_{RW}を備え、このアンテナL_{RW}に電流I_{RW}を流すことでその周辺に磁界を発生させる。一方、ＩＣカード側では、電気的にはＩＣカードの周辺にループ・コイルL_cが形設されている。ＩＣカード側のループ・コイルL_c端にはカード読み書き装置側のループ・アンテナL_cが発する磁界による誘導電圧が生じて、ループ・コイルL_c端に接続されたＩ

Ｃカードの端子に入力される。

【００４８】

カード読み書き装置側のアンテナL_{RW}とＩＣカード側のループ・コイルL_cは、その結合度は互いの位置関係によって変わるが、系としては１個のトランスを形成していると捉えることができ、ＩＣカードの読み書き動作を図２に示すようにモデル化することができる。

【００４９】

カード読み書き装置側では、アンテナL_{RW}に流す電流I_{RW}を変調することによって、ＩＣチップ上のループ・コイルL_cに誘起される電圧V_0は変調を受け、そのことを利用してカード読み書き装置はＩＣカードへのデータ送信を行なうことができる。

【００５０】

また、ＩＣカードは、カード読み書き装置へ返送するためのデータに応じてループ・コイルL_cの端子間の負荷を変動させる機能（Ｌｏａｄ Ｓｗｉｔｃｈｉｎｇ）を持つ。ループ・コイルL_cの端子間の負荷が変動すると、カード読み書き装置側ではアンテナ端子間のインピーダンスが変化して、アンテナL_{RW}の通過電流I_{RW}や電圧V_{RW}の変動となって現れる。この変動分を復調することで、カード読み書き装置はＩＣカードの返送データを受信することができる。

【００５１】

すなわち、ＩＣカードは、カード読み書き装置からの質問信号に対する応答信号に応じて自身のアンテナ間の負荷を変化させることによって、カード読み書き装置側の受信回路に現れる信号に振幅変調をかけて通信を行なうことができる訳である。

【００５２】

ＩＣカードは、カード型のデータ通信装置であってもよいし、いわゆるＩＣカード機能を有する集積回路チップを携帯電話機等の情報通信端末機器に内蔵してもよい（ＩＣカードが機器に内蔵される場合であっても、機器に着脱可能に構成される場合であっても、本明細書中では便宜上「ＩＣカード」と呼ぶ場合がある。）また、ＩＣカード機能を有する集積回路チップは、例えば携帯電話機やＰＤＡなどの携帯端末、あるいはパーソナルコンピュータ（ＰＣ）などの情報処理端末に搭載されて外部機器とデータ通信を行なう。この場合、リーダ／ライタ装置と有線あるいは無線で接続するためのインターフェース以外に、外部機器接続用のインターフェースを備えている。

【００５３】

図３には、本発明の実施形態にかかるデータ通信装置のハードウェア構成を示している。このデータ通信装置は、通信用のアンテナを追加して内部の不揮発性メモリにアクセスすることができるＩＣカード機能と、ＩＣカード機能を有する外部装置に電力を供給するとともにデータ交換を実現するリーダ／ライタ機能を有し、カード機能アナログ回路部３０、データ処理部４０と、リーダ／ライタ機能アナログ回路部５０を有するＩＣチップを内蔵している。同図に示した例では、ＩＣカードはカード読み書き機能も併せて備えているが、カード読み書き機能は本発明の必須の構成要素ではない。

【００５４】

カード機能アナログ回路部３０では、アンテナ３２で受信された搬送波は、整流器３１で整流された後、データ処理部４０内の信号処理部４４に供給されるとともに、シリアル・レギュレータ３３を介して論理回路３８に供給されている。

【００５５】

論理回路３８は、シリアル・レギュレータ３３からの電圧を制御して、ＩＣカードで使用するための適正な電源電圧V_{DD}を供給するようになっている。

【００５６】

シリアル・レギュレータ３３は、入力電圧の如何に拘わらず、出力電圧をほぼ一定に保つようになっている。すなわち、入力電圧が高いときには、内部インピーダンスを高くして、逆に入力電圧が低いときには内部インピーダンスを低くすることによって、電圧を保つ動作を可能とする。

【００５７】
電圧検出器３９は、論理回路３８に接続された外部電源（バッテリなど）の出力端子電圧を監視して、外部電源の電圧が所定電圧を下回った場合には外部電源の使用を禁止する信号を論理回路３８に出力するようになっている。
【００５８】
また、カード機能アナログ回路部３０において、アンテナ３２から入力された電波は、搬送波検出器３４で受信電波中に搬送波が含まれているか否かが判断され、含まれている場合には、搬送波検出信号ＶＲが論理回路３８に出力される。論理回路３８は、さらに、データ処理部４０に対して搬送波が検出された旨の信号を出力することができる。
【００５９】
クロック抽出器３５は、アンテナ３２から入力された電波からクロックを抽出して、これをクロック選択器３６に供給する。また、クロック発振器３７は、例えばＩＣカード外に配設された水晶振動子で構成され、ＩＣカード上で使用される駆動周波数のクロックを発生して、クロック選択器３６に供給する。クロック選択器３６は、クロック抽出器３５から供給されたクロック、又は、クロック発振器３７から供給されたクロックのいずれか一方を選択して、ＩＣカード内の各部に供給する。
【００６０】
リーダ／ライタ機能アナログ回路部５０は、送信アンプ５１と、受信信号検出器５３と、受信アンプ・フィルタ５４と、送受信用のアンテナ５２及び５５で構成される。
【００６１】
データを送信するときは、データ処理部４０の信号処理部４４によって変調並びにＤ／Ａ変換されて、アナログ・ベースバンドにアップコンバートされた送信信号が送信アンプを介してアンテナ５１から送出される。また、アンテナ５２から受信された信号は、受信信号検出器５３によって検出され、受信アンプ５４で増幅されてから、信号処理部４４に供給される。信号処理部４４は、アナログ・ベースバンド信号にダウンコンバートし、Ｄ／Ａ変換並びに復調処理して、ディジタル・データを再現する。
【００６２】
なお、ＩＣカードとカード読み書き装置の間のカード読み書き動作は、図１及び図２を参照しながら既に説明した通りである。
【００６３】
データ処理部４０は、先述の信号処理部４４の他、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）４５と、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）などを利用したデータ暗号化エンジン４６と、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）などを利用したエラー訂正部４７と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）４１と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）４２と、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ ａｎｄ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）４３と、ＵＡＲＴインターフェース４８と、I^2Cインターフェース４９とを備えており、各部は内部バスによって相互接続されている。
【００６４】
ＣＰＵ４５は、ＩＣカード内の動作を統括的に制御するメイン・コントローラであり、ＩＣカード用オペレーティング・システム（ＯＳ）によって提供される実行環境（後述）下で、例えばＲＯＭ４２（あるいはＥＥＰＲＯＭ４３）に格納されたプログラム・コードを実行するようになっている。例えば、ＣＰＵ４５は、カード機能アナログ回路部３０やリーダ／ライタ機能アナログ回路部４０を介して送受信されるデータに関するアプリケーションを実行するようになっている。
【００６５】
信号処理部４４は、カード機能アナログ回路部３０やリーダ／ライタ機能アナログ回路部４０を介して送信されるデータの変調、Ｄ／Ａ変換、アップコンバートなどの処理や、受信したデータのダウンコンバート、Ａ／Ｄ変換、復調などの処理を行なう。
【００６６】

ＤＥＳエンジン４６は、カード機能アナログ回路部３０やリーダ／ライタ機能アナログ回路部４０を介して送受信されるデータを手順公開型の秘密鍵暗号により暗号化及び復号化処理する。

【００６７】

ＣＲＣ４７は、カード機能アナログ回路部３０やリーダ／ライタ機能アナログ回路部４０を介して受信したデータの巡回冗長検査を行なう。

【００６８】

ＵＡＲＴ４８並びにI^2Cインターフェースは、ＩＣカードを携帯電話器やＰＤＡ、パーソナル・コンピュータなどの外部機器（図１１には図示しない）に接続するための外部有線インターフェースを構成する。このうちＵＡＲＴ（Ｕｎｉｖｅｒｓａｌ ａｓｙｎｃｈｒｏｎｏｕｓ ｒｅｃｅｉｖｅｒ ｔｒａｎｓｍｉｔｔｅｒ）４８は、コンピュータ内のパラレル信号をシリアル信号に変換したり、シリアル信号をパラレル信号に変換したりする機能を持つ。

【００６９】

ＲＡＭ４１は書き込み可能なメモリ装置であり、ＣＰＵ４１はＲＡＭ４１を作業領域としてプログラムを実行する。ＲＡＭ４１が提供するメモリ空間はアドレス可能であり、ＣＰＵ４１や内部バス上の各装置はこのメモリ空間にアクセスすることができる。

【００７０】

ＥＥＰＲＯＭ４３は、消去動作とともに新規のデータの書き込みを行なう不揮発性のメモリ装置である。本明細書で言うＩＣカード内蔵のメモリ領域は、基本的にはＥＥＰＲＯＭ４３内の書き込み可能領域を指すものとする。

【００７１】

このメモリ領域は、１以上のファイル・システムで構成される。初期状態では、元のＩＣカード発行者が管理する単一のファイル・システムによってメモリ領域が管理され、その後、ＩＣカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割する。ＥＥＰＲＯＭ４３上のメモリ領域のファイル分割や、分割後のアクセス動作の詳細については、後に詳解する。

【００７２】

図４には、本実施形態に係るＩＣカードにおけるメモリ領域の制御システム構成を模式的に示している。同図に示すように、この制御システムは、基本的には、オペレーティング・システム内のサブシステムとして実装され、プロトコル・インターフェース部と、ＯＳ中枢部と、ファイル・システムで構成される。

【００７３】

プロトコル・インターフェース部は、ＵＡＲＴ４８などの外部機器インターフェースを介した外部機器からのファイル・システムへのアクセス要求、あるいは非接触ＩＣカード・インターフェースを介したカード読み書き装置からファイル・システムへのアクセス要求のハンドリングを行なう。

【００７４】

ＯＳ中枢部では、ファイル・システムとやり取りするデータのデコード／エンコード、ＣＲＣなどによるエラー訂正、ＥＥＰＲＯＭ４３のブロック毎の書き換え回数管理、ＰＩＮ照合、相互認証などを行なう。

【００７５】

さらに、ＯＳ中枢部は、ファイル・アクセス時におけるＰＩＮ照合や相互認証、ファイルのリード／ライトなどのファイル・システムへの幾つかのＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）を備えている。

【００７６】

ファイル・システム・エンティティとしてのＥＥＰＲＯＭ４３へ物理アクセスを行なう。ＥＥＰＲＯＭなどのメモリ・デバイスへの物理アクセス動作自体は当業界において周知なので、ここでは説明を省略する。

【００７７】

ＥＥＰＲＯＭ４３上に展開されるメモリ領域は、１以上のファイル・システムで構成される。初期状態では、元のＩＣカード発行者が管理する単一のファイル・システムによってメモリ領域が管理されている。ＩＣカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割する際には、メモリ領域の分割権限と、元のＩＣカード発行者に対する認証の双方が要求される。そして、一旦分割されると、ファイル・システムへのアクセスは、元のＩＣカードの発行者ではなく、ファイル・システム自体のサービス提供元事業者への認証が要求される。ファイル・システムの分割は、仮想的なＩＣカードの発行である。

【００７８】

ＯＳは、分割を許可するための分割権限鍵K_dを管理している。また、ファイル・システム毎に、発行者（元のＩＣカード発行者、又はファイル分割した事業者）の発行者鍵K_Iと、システム・コードと、ファイル領域を識別するエリアＩＤが管理されている。

【００７９】

ファイル・システムへのアクセスは、ポーリングによるエリアＩＤの要求と、相互認証という手続きを経て行なわれる。ファイル・システムの発行者（元のファイル・システムの場合はカード発行者、分割後のファイル・システムを使用するサービス提供元事業者）は、まず、自身が判っているシステム・コードを引数にしてファイル・システムに対するポーリングを行なうことによって、該当するファイル・システムのメモリ領域上でのエリアＩＤを取得することができる。次いで、このエリアＩＤと発行者鍵K_Iを用いて相互認証を行なう。そして、相互認証が成功裏に終わると、ファイル・システムへのアクセスが許可される。ファイル・システムへのアクセスは、発行者と該当するファイル・システムに固有の発行者鍵K_Iを用いた暗号化通信により行なわれるので、他のファイル・システムが無関係のデータを取り込んだり、発行者以外がファイル・システムへ無断で読み書きしたりすることはできない。

【００８０】

図５には、比較的大容量のＩＣカードを用いて実現される、電子マネーや電子チケット、その他の価値情報を運用するサービス提供システムの全体的構成を模式的に示している。

【００８１】

図示のシステム１は、例えば、ＩＣカード発行者２１が使用する発行者用通信装置１１と、カード記憶領域運用者２２が使用する運用者用通信装置１２と、装置製造者２３が使用する製造者用通信装置１３と、カード記憶領域使用者２４が使用する記憶領域分割装置１４及び運用ファイル登録装置１５とで構成される。

【００８２】

システム１では、ＩＣカード発行者２１がカード所有者２６にＩＣカード１６を発行した場合に、所定の条件に基づいて、カード記憶領域使用者２４によって提供されるサービスに係わるファイル・データをＩＣカード１６に登録し、カード所有者２６が単体のＩＣカード１６を用いて、ＩＣカード発行者２１及びカード記憶領域使用者２４の双方のサービスを受けることを可能にするものである。

【００８３】

図１に示すように、システム１では、発行者用通信装置１１、運用者用通信装置１２、製造者用通信装置１３、記憶領域分割装置１４及び運用ファイル登録装置１５が、ネットワーク１７を介して接続される。

【００８４】

ＩＣカード発行者２１は、ＩＣカード１６の発行を行なう者であり、ＩＣカード１６を用いて自らのサービスを提供する。

【００８５】

カード記憶領域運用者２２は、ＩＣカード発行者２１からの依頼を受けて、ＩＣカード発行者２１が発行したＩＣカード１６内の記憶部（半導体メモリ）に構成される記憶領域のうち、ＩＣカード発行者２１が使用しない記憶領域をカード記憶領域使用者２４に貸し

出すサービスを行なう者である。

【００８６】

装置製造者２３は、カード記憶領域運用者２２から依頼を受けて、記憶領域分割装置１４を製造し、カード記憶領域使用者２４に納品する者である。

【００８７】

カード記憶領域使用者２４は、カード記憶領域運用者２２に依頼を行ない、ＩＣカード１６の記憶領域を使用して自らの独自のサービスを提供する者であり、メモリ領域を分割して新たなファイル・システムを作成するサービス提供元事業者（前述）に相当し、自己のファイル・システムを利用して自身のサービス提供を行なう。

【００８８】

カード所有者２６は、ＩＣカード発行者２１からＩＣカード１６の発行を受け、ＩＣカード発行者２１が提供するサービスを受ける者である。カード所有者２６は、ＩＣカード１６の発行後に、カード記憶領域使用者２４が提供するサービスを受けることを希望する場合には、記憶領域分割装置１４及び運用ファイル登録装置１５を用いて、カード記憶領域使用者２４のサービスに係わるファイル・データをＩＣカード１６に記憶し、その後、カード記憶領域使用者２４のサービスを受けることができるようになる。

【００８９】

システム１は、ＩＣカード発行者２１のサービスと、カード記憶領域使用者２４のサービスとを単体のＩＣカード１６を用いて提供するに当たって、ＩＣカード発行者２１及びカード記憶領域使用者２４のサービスに係わるファイル・データが記憶される記憶領域に、権限を有しない他人によって不正にデータの書き込み及び書き換えなどが行なわれることを困難にする構成を有している。

【００９０】

ＩＣカード１６は、その字義通り、カード型のデータ通信装置であってもよいし、いわゆるＩＣカード機能が実装された半導体チップを内蔵した携帯電話機（あるいはその他の携帯端末）として具現化されることもある。

【００９１】

なお、図５では、それぞれ単数のＩＣカード発行者２１、カード記憶領域使用者２４及びカード所有者２６がある場合を例示したが、これらは、それぞれ複数であってもよい。

【００９２】

本実施形態では、ＩＣカードの単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のデータ通信装置を複数の事業者で共有し、単一のデータ通信装置により複数のサービスを提供する。このような分割ファイル・システム構成により、元のカード発行者が利用するメモリ領域の他に、元のカード発行者の許可を得て特定のサービス提供元事業者が利用可能となるメモリ領域と、元のカード発行者の許可を得て複数の事業者間で共通に利用可能となるメモリ領域を運用することができる。

【００９３】

特に、元のカード発行者が利用するファイル・システム以外に、各サービス提供元事業者が個別に利用可能となる１以上のファイル・システムを運用する場合、ファイル・システム間の境界がファイヤ・ウォールとして機能し、他のファイル・システム（すなわち他のサービス提供元事業者）からのアクセス（不正侵入）を好適に排除することができる。

【００９４】

ここで、図６～図９を参照しながら、ＩＣカード内のメモリ領域の運用形態について説明する。

【００９５】

図６には、元のカード発行者が自らのファイル・システムのみを管理しているメモリ領域の状態を示している。元のカード発行者のシステム・コードＳＣ１は、システム・コードの管理機構が付与する。外部機器又はプログラムがカード発行者のファイル・システムにアクセスする場合は、ＳＣ１を識別コード（すなわち、要求コマンドの引数）とする。

【００９６】

図７には、カード発行者が自らのファイル・システムの空き領域の内で、ある範囲のメモリを領域管理者に貸与（又は譲渡）することが許可できることを示している。この段階では，まだメモリ領域上のファイル・システムに対して分割が行なわれている訳ではない。カード発行者は、自らのファイル・システムに空き領域はあるうちは、複数の領域管理者に対して、メモリを貸与することを許可できる。例えば、４ビットのシステム・コードでファイル・システムを識別するという実装では、最大１６分割（１５回まで分割）することができる。

【００９７】

図８には、他のサービス提供元事業者が、カード発行者から許可された領域においてメモリ領域を分割し、新たなファイル・システムを生成した状態を示している。この新規ファイル・システムには、システム・コードの管理機構からシステム・コードＳＣ２が付与されている。外部機器又はプログラムが、当該メモリ領域管理者（サービス提供元事業者）の運用するファイル・システムにアクセスする場合は、ＳＣ２を識別コード（要求コマンドの引数）とする。

【００９８】

図９には、共通領域管理者が、カード発行者から許可された領域において、共通領域のシステム・コードＳＣ０でメモリを分割した状態を示している。外部機器又はプログラムがこの共通領域管理者の運用領域であるファイル・システムにアクセスする場合には、そのシステム・コードＳＣ０を識別コード（要求コマンドの引数）とする。

【００９９】

図６に示した初期のメモリ領域の状態から、他のサービス提供元事業者用のファイル・システムを分割するためには、当該事業者は、カード発行者に対してメモリ領域の使用に関する許可を求める。そして、カード発行者はメモリ領域の使用、すなわちファイル・システムの分割を許可する場合には、分割技術管理者から、ファイル・システムの分割に必要となる「分割素パッケージ」を取得する。カード発行者は、取得した分割素パッケージと、新たなサービス提供元事業者に使用を許可する分割領域の大きさ（ブロック数）とからなるデータ・ブロックをさらに自己の発行者鍵K_Iで暗号化して、分割パッケージを作成し、これを用いてファイル・システムの分割要求を行なう。

【０１００】

但し、メモリ領域を分割して新たなファイル・システムを作成する手順自体は本発明の要旨ではないので、ここではこれ以上説明しない。

【０１０１】

図１０には、分割操作の繰り返しにより、ＩＣカードのメモリ領域上に複数のファイル・システムが共存するメモリ空間の構造を模式的に示している。

【０１０２】

図示の通り、ファイル・システム毎にシステム・コードＳＣとエリアＩＤが設定されるとともに、当該領域を使用するサービス提供元事業者（元のカード発行者を含む）の発行者鍵K_Iで相互認証を行なうことができる。これによって、ファイル・システムが割り振られたサービス提供元事業者は、元のカード発行者や分割技術者とは独立して、自己のファイル・システムのセキュリティに関する脅威を分析、管理、並びに運用することができる。

【０１０３】

また、サービス提供元事業者が自己のファイル・システムへアクセスする際には、基本的には、エリアＩＤの要求と、相互認証という手続きを経て行なわれる。まず、自身が判っているシステム・コードを引数にしてファイル・システムに対するポーリングを行なうことによって、該当するファイル・システムのメモリ領域上でのエリアＩＤを取得することができる。次いで、このエリアＩＤと発行者鍵K_Iを用いて相互認証を行なう。そして、相互認証が成功裏に終わると、ファイル・システムへのアクセスが許可される。

【０１０４】

図１１には、外部機器とＩＣカードの間で交換される要求コマンドの構造を模式的に示

している。図示の通り、各サービス提供元事業者（元のカード発行者を含む）は、要求コマンド（例えばリード要求やライト要求、データ消去要求、エリア／サービス登録（後述）など）は、事業者自身と該当するファイル・システムに固有の発行者鍵K_Iを用いてパッケージ化して暗号化通信により行なわれる。したがって、他のファイル・システムが要求コマンドから無関係のデータを取り込んだり、第３者がファイル・システムへ無断で読み書きしたりすることはできない。

【０１０５】

ＩＣカードのメモリ領域は、分割操作を繰り返すことにより、図１０に示すように複数のファイル・システムが共存する構造となる。元のカード発行者の許可によりＩＣカード上で自己のファイル・システムを取得したサービス提供元事業者は、それぞれ自己のファイル・システムを利用してエリアやサービスを配設し（後述）、自らＩＣカードの発行者であるかのように、自身の事業展開に利用することができる。

【０１０６】

以下では、１つのファイル・システム内での運用形態について説明する。基本的には、どのファイル・システムにおいても同様の動作が実現されるものとする。また、ファイル・システムの操作を行なうためには、ポーリングによるエリアＩＤの要求と、相互認証という手続き（前述）を経ていることを前提とする。

【０１０７】

ファイル・システム内には、電子決済を始めとする外部との電子的な価値情報のやり取りなど、１以上のアプリケーションが割り当てられている。アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ。また、アプリケーションの利用、すなわち該当するサービス・メモリ領域へアクセスする処理動作のことを「サービス」と呼ぶ。サービスには、メモリへの読み出しアクセス、書き込みアクセス、あるいは電子マネーなどの価値情報に対する価値の加算や減算などが挙げられる。

【０１０８】

ユーザがアクセス権を持つかどうかに応じてアプリケーションの利用すなわちサービスの起動を制限するために、アプリケーションに対して暗証コードを割り当て、サービス実行時に暗証コードの照合処理を行なうようになっている。また、サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

【０１０９】

ユーザがアクセス権を持つかどうかに応じてアプリケーションの利用すなわちサービスの起動を制限するために、アプリケーションに対して暗証コードすなわちＰＩＮを割り当て、サービス実行時にＰＩＮの照合処理を行なうようになっている。また、サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

【０１１０】

本実施形態では、ＩＣカード内のメモリ領域に設定されているそれぞれのファイル・システムに対して、「ディレクトリ」に類似する階層構造を導入する。そして、メモリ領域に割り当てられた各アプリケーションを、所望の階層の「エリア」に登録することができる。例えば、一連のトランザクションに使用される複数のアプリケーション、あるいは関連性の深いアプリケーション同士を同じエリア内のサービス・メモリ領域として登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことによって、メモリ領域のアプリケーションやエリアの配置が整然とし、ユーザにとってはアプリケーションの分類・整理が効率化する。

【０１１１】

また、ファイル・システムへのアクセス権を階層的に制御するために、アプリケーション毎にＰＩＮを設定できる以外に、各エリアに対してもＰＩＮを設定することができるようにしている。例えば、あるエリアに該当するＰＩＮを入力することにより、照合処理並びに相互認証処理を経て、エリア内のすべてのアプリケーション（並びにサブエリア）へ

のアクセス権を与えるようにすることもできる。したがって、例えば、該当するエリアに対するＰＩＮの入力を１回行なうだけで、一連のトランザクションで使用されるすべてのアプリケーションのアクセス権を得ることができるので、アクセス制御が効率化するとともに、機器の使い勝手が向上する。

【０１１２】

さらに、あるサービス・メモリ領域に対するアクセス権限が単一でないことを許容し、それぞれのアクセス権限毎、すなわちサービス・メモリ領域において実行するサービスの内容毎に、暗証コードを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々のＰＩＮが設定される。また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々のＰＩＮが設定される。また、あるメモリ領域に対する読み出しについてはＰＩＮの入力が必要でないが、書き込む場合にはＰＩＮの入力を必須とさせることが可能である。

【０１１３】

図１２には、ファイル・システム内のデータ構造例を模式的に示している。図示の例では、ファイル・システムが持つ記憶空間には、「ディレクトリ」に類似する階層構造が導入されている。すなわち、メモリ領域に割り当てられた各アプリケーションを、所望の階層エリアにサービス・メモリ領域として登録することができる。例えば、一連のトランザクションに使用されるアプリケーションなど、関連性の深いアプリケーション同士を同じエリアに登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことができる。

【０１１４】

また、ファイル・システム内に割り当てられたアプリケーション（すなわちサービス・メモリ領域）並びにエリアは暗証コード定義ブロックを備えている。したがって、アプリケーション毎に、あるいはエリア毎にＰＩＮを設定することができる。また、ファイル・システムに対するアクセス権は、アプリケーション単位で行なうとともに、並びにエリア単位で行なうことができる。

【０１１５】

さらに、あるサービス・メモリ領域に対するアクセス権限が単一でなく、実行するサービスの内容毎に、ＰＩＮを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々のＰＩＮが設定され、また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々のＰＩＮが設定される。

【０１１６】

照合部は、例えば電磁誘導作用に基づく非接触近距離通信又はＵＡＲＴ４８やＩ^{2}Ｃ４９などのプロトコル・インターフェースを介して送られてくるＰＩＮを、各アプリケーション又はディレクトリに割り当てられたエリア又はサービス・メモリ領域に設定されている暗証コードと照合して、一致するメモリ領域に対するアクセスを許可する。アクセスが許可されたメモリ領域は、プロトコル・インターフェースを介して読み書きが可能となる。

【０１１７】

このようにファイル・システム内には、アプリケーションに割り当てられたさまざまなサービス・メモリ領域が割り当てられており、各サービス・メモリ領域に対して適用可能な１以上のサービスが設けられている。本実施形態では、エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、アプリケーションに適用されるサービスの種類毎にＰＩＮを設定して、サービス単位でアクセス制限を行なうことができる。

【０１１８】

図１３には、ファイル・システムの基本構成を示している。図１２を参照しながら既に説明したように、ファイル・システムに対して、「ディレクトリ」に類似する階層構造が導入され、所望の階層のエリアに、アプリケーションに割り当てられたサービス・メモリ

領域を登録することができる。図１３に示す例では、エリア００００定義ブロックで定義されるエリア００００内に、１つのサービス・メモリ領域が登録されている。

【０１１９】

図示のサービス・メモリ領域は、１以上のユーザ・ブロックで構成される。ユーザ・ブロックはアクセス動作が保証されているデータ最小単位のことである。このサービス・メモリ領域に対しては、サービス０１０８定義ブロックで定義されている１つのサービスすなわちサービス０１０８が適用可能である。

【０１２０】

エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、サービスの種類毎に暗証コードを設定して、サービス単位でアクセス制限を行なうことができる。アクセス制限の対象となるサービスに関する暗証コード設定情報は、暗証コード専用のサービス（すなわち「暗証コード・サービス」）として定義される。図１３に示す例では、サービス０１０８に関する暗証コードが暗証コード・サービス０１２８定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

【０１２１】

サービス０１０８に対する暗証コード・サービスが有効になっている場合、サービス０１０８を起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なう前に、暗証コード・サービス０１２８を使用した暗証コードの照合が必要となる。具体的には、暗号化あり読み書き（Ｒｅａｄ／Ｗｒｉｔｅ）コマンドを使用する場合は、相互認証前にサービス０１０８に対する暗証コードすなわちＰＩＮの照合を行なう。

【０１２２】

また、アプリケーションに割り当てられたサービス・メモリ領域を所望の階層のエリアに登録するとともに、エリアを階層化する（関連性の深いエリア同士を同じ親エリアに登録する）ことができる。この場合、エリア毎にＰＩＮを設定することにより、エリアをアクセス制限の単位とすることができる。図１４には、ＩＣカード５０のメモリ空間においてエリアが階層化されている様子を示している。同図に示す例では、エリア０００００定義ブロックで定義されているエリア００００内に、エリア１０００定義ブロックで定義されている別のエリア１０００が登録されている。

【０１２３】

図１４に示す例では、さらにエリア１０００内には、２つのサービス・メモリ領域が登録されている。一方のサービス・メモリ領域に対しては、サービス１１０８定義ブロックで定義されているサービス１１０８と、サービス１１０Ｂ定義ブロックで定義されているサービス１１０Ｂが適用可能である。このように、１つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義することを、本明細書中では「オーバーラップ・サービス」と呼ぶ。オーバーラップ・サービスにおいては、同じサービス・エリアに対して、入力したＰＩＮに応じて異なるサービスが適用されることになる。また、他方のサービス・メモリ領域に対しては、サービス１１０Ｃ定義ブロックで定義されているサービス１１０Ｃが適用可能である。

【０１２４】

各サービス・メモリ領域に設定されているサービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことができる。勿論、図１３を参照しながら説明したように、サービス毎に暗証コード・サービスを定義することができる。この場合、サービスに対する暗証コード・サービスが有効になっているときには、暗証コード・サービスを使用したＰＩＮの照合を行なってからサービスの起動が許可される。

【０１２５】

また、複数のサービスに対して共通のＰＩＮを設定したい場合には、これらサービスを含むエリアを作成し、このエリアに対して共通の暗証コード・サービスを適用することができる。

【０１２６】

図１４に示す例では、エリア１０００に関する暗証コードが、暗証コード・サービス１０２０定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

【０１２７】

エリア１０００に対する暗証コード・サービスが有効（後述）になっている場合、暗証コード・サービス１０２０を使用した暗証コードの照合を行なった後に、エリア１０００内の各サービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことが可能となる。

【０１２８】

ここで、エリア１０００内のサービスに暗証コード・サービスが適用されており且つこれが有効となっている場合には、さらにその暗証コード・サービスを使用した暗証コードの照合を経てからでないと、そのユーザ・ブロックに読み出し又は書き込み動作を行なうことはできない。

【０１２９】

図１３及び図１４に例示したように、暗証コード照合の対象となるエリアやサービスに対応する暗証コード・サービスは一意に与えられる。

【０１３０】

なお、ファイル・システム内にエリアやサービスを登録するための手順自体は本発明の要旨に直接関連しないので、ここでは説明を省略する。

【０１３１】

図１３及び図１４に例示したように、ファイル・システム内に登録されたエリアやサービスに対してＰＩＮを適用して、エリア単位、あるいはサービス単位でアクセス制御を行なうことができる。また、１つのサービス・メモリ領域に対して複数のサービス（オーバーラップ・サービス）を登録することができるが、サービス毎にＰＩＮを適用することで、同じサービス・メモリ領域に対して複数のアクセス方法を定義することができる。

【０１３２】

但し、本実施形態では、ファイル・アクセスへアクセスする際、発行者鍵を用いた相互認証処理（前述）は必須であるが、ＰＩＮ照合処理は任意である。すなわち、サービス又はエリアに対する暗証コード・サービスが有効になっている場合にのみ、サービスの起動又はエリアへのアクセスを行なう前に、暗証コードの照合が要求され、暗証コード・サービスが無効にされている場合には、ＰＩＮの照合は要求されない。

【０１３３】

ＰＩＮの適用内容は、暗証コード・サービス定義ブロックの暗証コード・サービス・データ・ブロックに記述されている。図１５には、暗証コード・サービス・データ・ブロックのデータ構造を模式的に示している。同図に示すように、暗証コード定義領域は、暗証番号領域と、入力失敗回数記憶領域と、最大許容入力失敗回数設定領域と、暗証番号使用選択領域と、アクセス許可フラグとで構成されている。

【０１３４】

ユーザが入力したＰＩＮが一致した場合にのみ、該当するサービス又はエリアの暗証コード・サービス・データ・ブロック内のアクセス許可フラグを立てて、其処へのアクセスを許可する。

【０１３５】

アクセス許可フラグは、該当するアプリケーション又はディレクトリのアクセス可否状態を示すためのフラグであり、アクセス許可フラグが設定されたサービス又はエリアはアクセス許可状態である。ＰＩＮが設定されたサービスやエリアのアクセス許可フラグは、デフォルトではアクセス不可状態であり、ＰＩＮ照合処理及びファイル・システムの発行者鍵を用いた相互認証処理に成功した後、アクセス許可フラグが設定されて、アクセス許可状態に転じる。また、アクセス許可フラグを設定し続けると、ＩＣカードが紛失した場合や盗難に遭った場合にサービスやエリアの無断使用・不正使用によりユーザが損害を被るおそれがある。このため、ＩＣカードは、例えば電磁波が途絶えたことに応答してアク

セス許可状態を自動的にアクセス不可にする機構を備えていてもよい。

【０１３６】

また、誤ったＰＩＮが入力された場合には、その都度、入力失敗回数記憶領域の記録を更新する。そして、入力失敗回数が最大許容入力失敗回数設定領域に設定された最大許容入力失敗回数に到達した場合には、該当するサービスの起動又はエリアに対するアクセスを禁止する。

【０１３７】

一般には、この入力失敗回数は、一度入力に成功したらクリアするべきものである。このようにして悪意あるユーザがしらみつぶしに暗証コードを調べることを防止する。また、ユーザが誤って最大許容入力失敗回数に達して暗証コード入力に失敗してしまった場合は、ＩＣカードを管理する管理者（例えば分割技術管理者や元のカード発行者）のみが入力失敗回数記憶領域をクリアできるようにしてもよい。この管理者の認証には、例えば後述するような秘密鍵による認証を使用することもできる。

【０１３８】

図１６には、ユーザから入力された暗証コードに従って、サービスの起動又はエリアへのアクセス権を制御するための処理手順をフローチャートの形式で示している。

【０１３９】

ユーザから暗証コードを入力すると（ステップＳ１１）、各暗証コード・サービス定義ブロックの暗証コード・サービス・データ・ブロックにアクセスして、暗証コードが一致するか否かを判別する（ステップＳ１２）。

【０１４０】

暗証コード・サービス・データ・ブロックのＰＩＮがユーザ入力されたＰＩＮと一致する場合には、その暗証コード・サービス・データ・ブロック内のアクセス許可フラグを設定して、対応するサービス又はエリアをアクセス可能状態にする（ステップＳ１３）。

【０１４１】

例えば、ＩＣチップをリーダ／ライタにかざして、リーダ／ライタに接続されている外部機器（図示しない）のユーザ・インターフェースを用いて入力されたＰＩＮを、電磁誘導作用に基づく非接触近距離通信インターフェースでＩＣカードに送信することができる。

【０１４２】

図１６に示すようにＰＩＮを用いてアプリケーションやディレクトリへのアクセス権を制御する場合、悪意のあるユーザはしらみつぶしにＰＩＮを調べることにより、セキュリティの壁が破られる可能性がある（特に桁数の少ない暗証コードを用いる場合）。このため、本実施形態では、暗証コード定義領域において、最大許容入力回数を設定して、入力失敗回数が最大許容入力回数に到達したアプリケーション又はディレクトリをアクセス不可状態に設定することで、アクセス制御を行なうようにしている。

【０１４３】

図１７には、ＰＩＮの入力失敗回数によりサービスやエリアへのアクセス権制御を行なうための処理手順をフローチャートの形式で示している。

【０１４４】

ユーザからＰＩＮを入力すると（ステップＳ２１）、各暗証コード・サービス定義ブロックにアクセスして、ＰＩＮが一致するか否かを判別する（ステップＳ２２）。

【０１４５】

ユーザ入力されたＰＩＮが暗証コード・サービス定義ブロックのＰＩＮと一致する場合には、その暗証コード・サービス・データ・ブロック内のアクセス許可フラグを設定して、該当するサービス又はエリアをアクセス可能状態にする（ステップＳ２３）。

【０１４６】

他方、ユーザ入力されたＰＩＮがいずれの暗証コード・サービス定義ブロックのＰＩＮとも一致しない場合には、暗証コード定義領域内の入力失敗回数を更新する（ステップＳ２４）。また、ユーザ入力されたＰＩＮがいずれの暗証コード・サービス定義ブロックの

ＰＩＮと一致し、照合に成功した場合には、入力失敗回数を０にクリアする。

【０１４７】

そして、ステップＳ２５では、更新された入力失敗回数が、暗証コード定義領域内で設定されている最大許容入力回数に到達したか否かを判断する（ステップＳ２５）。

【０１４８】

もし、入力失敗回数が最大許容入力回数に到達してしまったならば、その暗証コード定義領域内のアクセス許可フラグの設定を解除して、該当するサービス又はエリアをアクセス不可状態にする（ステップＳ２６）。この結果、悪意のあるユーザがしらみつぶしにＰＩＮを調べる行為を取り締まることができる。

【０１４９】

また、ユーザが誤って最大許容入力失敗回数に達して暗証コード入力に失敗してしまった場合は、ＩＣカードを管理する管理者（例えば、分割技術管理者、または元のカード発行者）のみが入力失敗回数記憶領域をクリアできるようにしてもよい。この管理者の認証には、例えば秘密鍵による認証を使用することもできる。

【０１５０】

上述したように、本実施形態では、ファイル・システム毎に管理し、各ファイル・システムのセキュリティに関する脅威を分析、管理、並びに運用するようになっている。

【０１５１】

例えば、電磁誘導に基づく非接触近況通信インターフェース、あるいはＵＡＲＴ４８やI^2C４９などの有線インターフェースを介して、あるファイル・システムへのアクセスが行なわれると、当該ファイル・システムの発行者鍵K_Iを用いた相互認証、並びにＰＩＮ照合処理が行なわれ、これらの処理手続きに成功すると当該ファイル・システムは解除状態となり、読み／書きなど許可されたアクセス動作が可能となる。発行者鍵を用いた相互認証処理（前述）は必須であるが、ＰＩＮ照合処理は任意であり、ＰＩＮ照合が有効化されている場合のみその照合処理を行なう。また、認証・照合処理が成功裏に終わり、ファイル・システムが解除状態になった場合であっても、ファイル・システム内のエリアやサービスに個別のＰＩＮ照合が設定されている場合には、さらに逐次的にＰＩＮ照合処理が要求される。

【０１５２】

ここで、ＩＣカードのメモリ領域がサービス提供元事業者毎の複数のファイル・システムに分割され共用されるシステムにおいては、あるファイル・システムへのアクセスを試み、相互認証処理並びにＰＩＮ照合処理を経て、解除状態となりセッションが確立した際、この解除状態における他のファイル・システムのセキュリティへの影響が問題となる。何故ならば、セッションの状態が保たれると、その間、他のファイル・システムへのクラッキングの脅威があるからである。

【０１５３】

そこで、本実施形態では、ＩＣカードのメモリ領域に複数のファイル・システムを分割する機能と、各ファイル・システム上のディレクトリやファイルに対する暗証コードの照合機能を連携させることにより、ファイル・システム毎に独立してセキュリティに関する脅威を分析、管理、並びに運用するようにした。

【０１５４】

すなわち、ＩＣカードのメモリ領域上に、論理的に複数のファイル・システムが配置されている状態で（例えば、図１０を参照のこと）、外部機器又はプログラムがアクセス先のファイル・システムを変更したとき、各メモリ領域が保持しているシステム管理情報（相互認証情報を含む）やＰＩＮ の解除情報などをリセットする。さらに、ＩＣカードへの電源投入後、一定時間（例えば、利用時期のクラッキング技術やコンピュータの処理速度から、利用しているセッション暗号スキームを絶対に解読することができない時間）が経過した後、電源をリセットすることで、同様の相互認証・ＰＩＮ照合情報をリセットする。

【０１５５】

図１８には、ＩＣカード用のオペレーティング・システム（図４を参照のこと）で管理されている、相互認証・ＰＩＮ照合情報の状態遷移を示している。

【０１５６】

システム電源投入時、若しくはＯＳブート後は、ファイル・システムへのアクセス時に相互認証とＰＩＮ照合が求められる認証状態となる。但し、発行者鍵を用いた相互認証処理（前述）は必須であるが、ＰＩＮ照合処理は任意であり、ＰＩＮ照合が有効化されている場合のみその照合処理が求められる。

【０１５７】

ここで、電磁誘導に基づく非接触近況通信インターフェース、あるいはＵＡＲＴ４８やI^2C４９などの有線インターフェースを介して、外部機器又はプログラムとの間で相互認証が行なわれ、さらにＰＩＮ照合処理が行なわれ、これらの処理が成功裏に終了すると、システムは解除状態となり、読み／書きなど許可されたアクセス動作が可能となる。

【０１５８】

解除状態では、ＩＣカードへの電源投入後、一定時間（例えば、利用時期のクラッキング技術やコンピュータの処理速度から、利用しているセッション暗号スキームを絶対に解読することができない時間）が経過した後、電源をリセットすることで、認証状態へ復帰する。

【０１５９】

また、あるファイル・システムにおいて解除状態となった後、他のファイル・システムへの切り替えがなされたときにも、認証状態へ復帰する。ファイル・システムを切り替える際には、そのエリアＩＤを取得するためのポーリング手続きが必要となるので、オペレーティング・システムはこれを検知することができ、エリアＩＤを返す前に相互認証を実行する（前述）。

【０１６０】

このように、システムが認証状態と解除状態を適宜切り替えることにより、セッションの状態が保たれることによるクラッキングの脅威を排除することができる。

【０１６１】

ここで、図１９～図２１を参照しながら、ＩＣカード内のメモリ領域におけるシステム管理とＰＩＮ機能管理の連携について説明する。但し、各図ではメモリ領域は３つのファイル・システムに分割されているものとする。

【０１６２】

図１９には、メモリ領域の初期（すなわちリセット直後）の状態を示している。各ファイル・システムは、外部機器又はプログラムがアクセスするための識別子であるシステム・コードＳＣと、システム管理情報（相互認証情報を含む）、ＰＩＮ解除情報などを保持することができる。

【０１６３】

図２０には、外部機器又はプログラムがファイル・システム＃１に対して識別子ＳＣ１を用いてアクセスした際のメモリの状態を示している。外部機器又はプログラムは、戻り値としてエリアＩＤを受け取ることができる。ファイル・システム＃１がアクティブになると、セキュリティ情報でもあるシステム管理情報＃１及びＰＩＮ解除情報＃１がメモリ領域に保持される。

【０１６４】

図２１には、図２０に示した状態から、外部機器又はプログラムがファイル・システム＃２に対してシステム・コードＳＣ２を用いてアクセスした直後のメモリの状態を示している。この場合、ファイル・システムの切り替えが発生する。

【０１６５】

アクティブなファイル・システムの切り換えは、すべての論理的な機能の中で、最も優先して行なわれる。ファイル・システム＃２がアクティブになると同時に、ファイル・システム＃１がアクティブであったときにメモリ領域上に保持されていたシステム管理情報＃１及びＰＩＮ解除情報＃１は消去され、これに代わってシステム管理情報＃２、及びＰ

ＩＮ解除情報＃２　がメモリに保持される。

【０１６６】

このように、物理的なメモリ領域を複数のファイル・システムに分割する機能と、各ファイル・システム上のディレクトリやファイルに対するＰＩＮ 機能とを連携させて考えることで、ファイル・システム毎に安全に管理・運用することができるようになる。

【産業上の利用可能性】

【０１６７】

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

【０１６８】

本明細書では、ＩＣカードに内蔵されているメモリ領域についての情報管理方法を例にとって本発明の一実施形態について説明してきたが、本発明の要旨はこれに限定されるものではなく、ＩＣカード以外の機器に内蔵されている単一のメモリ・デバイスにおけるセキュリティの管理にも同様に適用することができる。

【０１６９】

要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【図面の簡単な説明】

【０１７０】

【図１】図１は、電磁誘導に基づくカード読み書き装置とＩＣカードとの無線通信の仕組みを概念的に示した図である。

【図２】図２は、カード読み書き装置とＩＣカードからなる系を１個のトランスとして捉えてモデル化した図である。

【図３】図３は、本発明の実施形態に係るデータ通信装置のハードウェア構成を示した図である。

【図４】本発明の一実施形態に係るＩＣカードにおけるメモリ領域の制御システム構成を模式的に示した図である。

【図５】図５は、ＩＣカードを用いたサービス提供システムの全体的構成を模式的に示した図である。

【図６】図６は、元のカード発行者が自らのファイル・システムのみを管理しているメモリ領域の状態を示した図である。

【図７】図７は、カード発行者が自らのファイル・システムの空き領域の内で、ある範囲のメモリを領域管理者に貸与（又は譲渡）することが許可できることを示した図である。

【図８】図８は、他のサービス提供元事業者が、カード発行者から許可された領域においてメモリ領域を分割し、新たなファイル・システムを生成した状態を示した図である。

【図９】図９は、共通領域管理者が、カード発行者から許可された領域において、共通領域のシステム・コードＳＣ０でメモリを分割した状態を示した図である。

【図１０】図１０は、分割操作の繰り返しにより、ＩＣカードのメモリ領域上に複数のファイル・システムが共存するメモリ空間の構造を模式的に示した図である。

【図１１】図１１は、外部機器とＩＣカードの間で交換される要求コマンドの構造を模式的に示した図である。

【図１２】図１２は、ファイル・システム内のディレクトリ構造例を模式的に示した図である。

【図１３】図１３は、ファイル・システムの基本構成を示した図である。

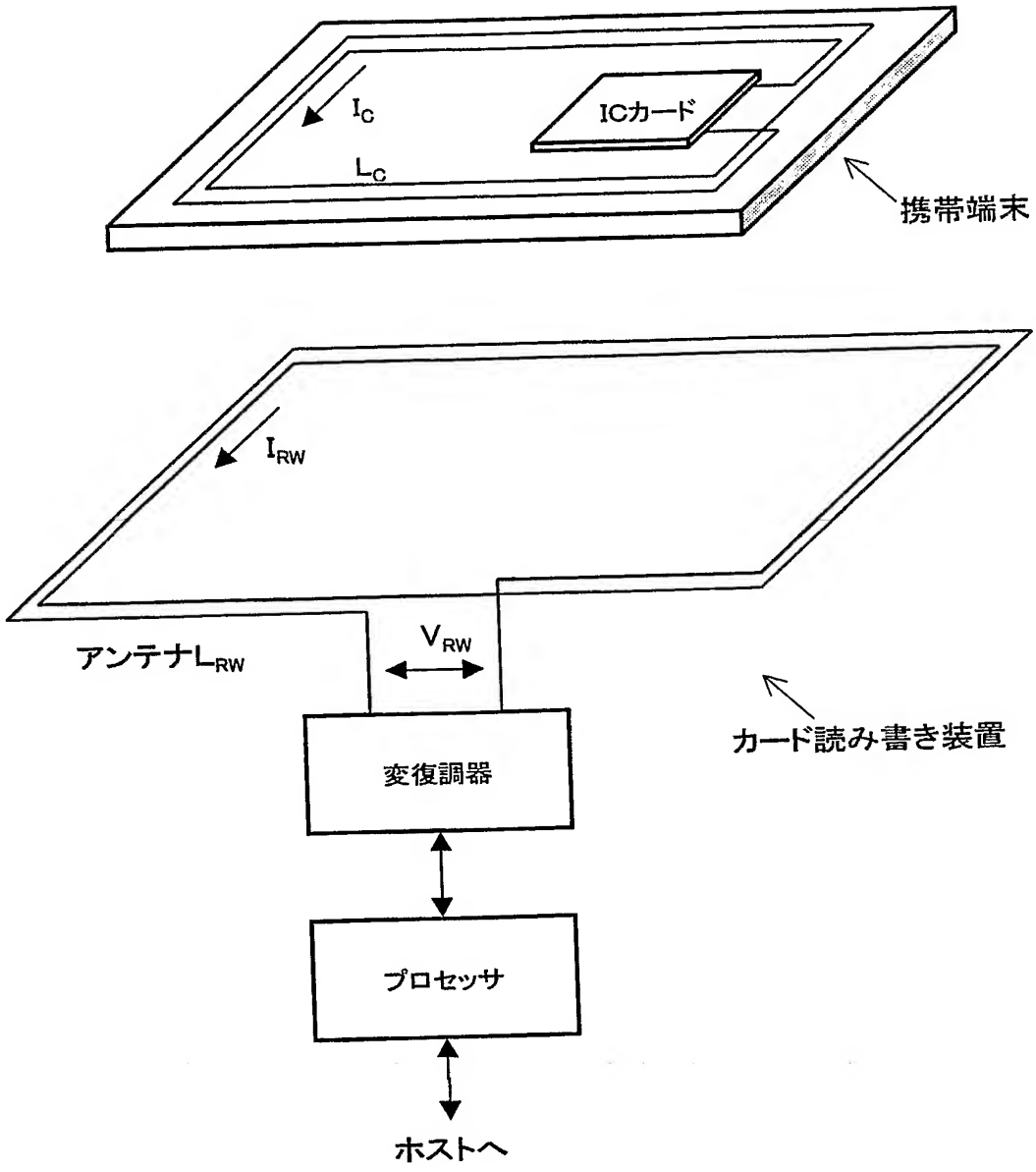
【図１４】図１４は、ＩＣカード５０のメモリ空間においてエリアが階層化されている様子を示した図である。

【図１５】図１５は、暗証コード・サービス・データ・ブロックのデータ構造を模式的に示した図である。
【図１６】図１６は、ユーザから入力された暗証コードに従って、サービスの起動又はエリアへのアクセス権を制御するための処理手順を示したフローチャートである。
【図１７】図１７は、ＰＩＮの入力失敗回数によりサービスやエリアへのアクセス権制御を行なうための処理手順を示したフローチャートである。
【図１８】図１８は、ＩＣカード用のオペレーティング・システム（図４を参照のこと）で管理されている、相互認証・ＰＩＮ照合情報の状態遷移を示した図である。
【図１９】図１９は、複数のファイル・システムに分割されたメモリ領域の初期の状態を示した図である。
【図２０】図２０は、外部機器又はプログラムがファイル・システム＃１に対して識別子ＳＣ１を用いてアクセスした際のメモリの状態を示した図である。
【図２１】図２１は、図２０に示した状態から、外部機器又はプログラムがファイル・システム＃２に対してシステム・コードＳＣ２を用いてアクセスした直後のメモリの状態を示した図である。

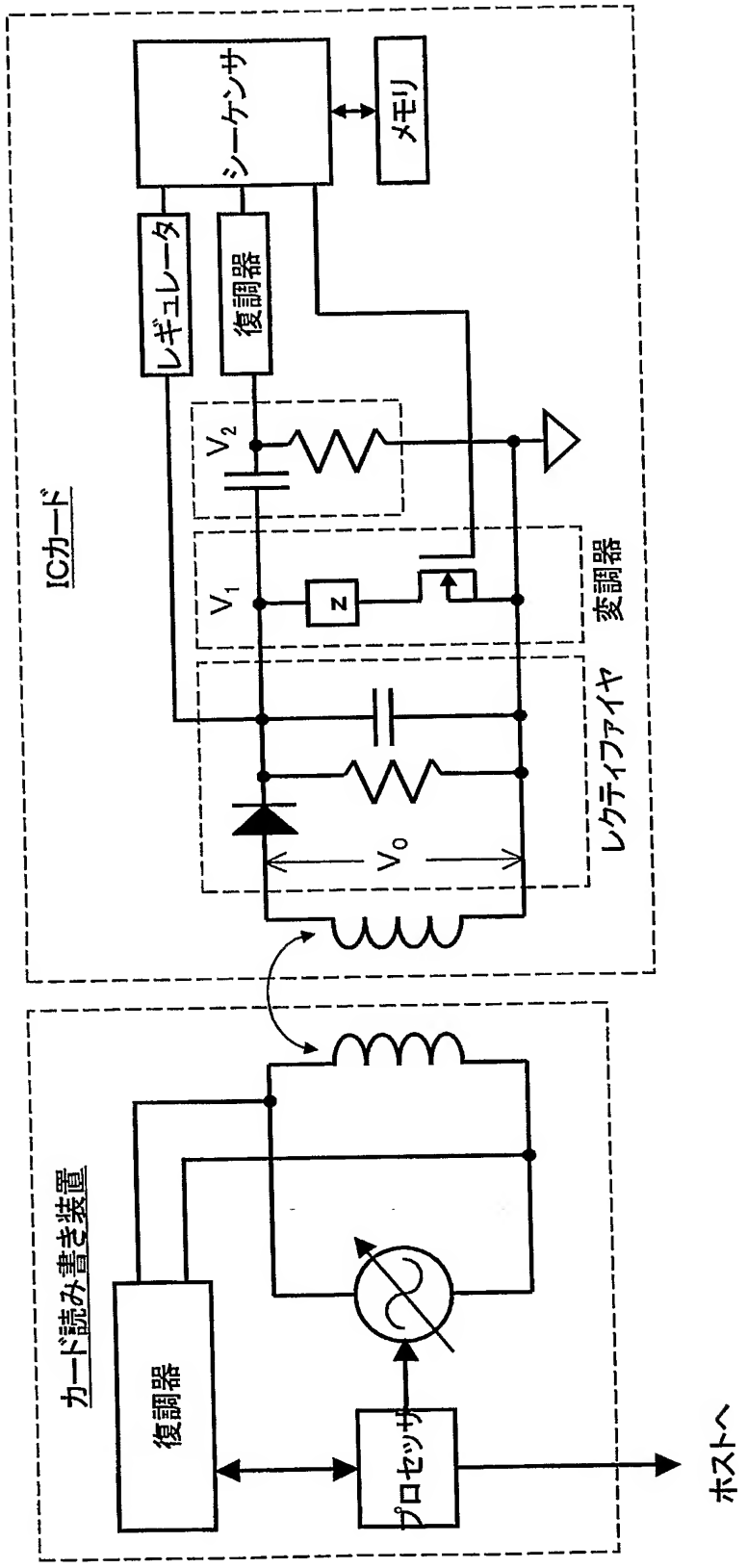
【符号の説明】
【０１７１】
１１…発行者用通信装置
１２…運用者要通信装置
１３…製造者用通信装置
１４…記憶領域分割装置
１５…運用ファイル登録装置
１６…ＩＣカード
１７…ネットワーク
２１…カード発行者
２２…カード記憶領域運用者
２３…装置製造者
２４…カード記憶領域使用者
２６…カード所有者
３０…カード機能アナログ回路部
３１…整流器
３２…アンテナ
３３…シリアル・レギュレータ
３４…搬送波検出器
３５…クロック抽出器
３６…クロック選択器
３７…クロック発振器
３８…論理回路
３９…電圧検出器
４０…データ処理部
４１…ＲＡＭ
４２…ＲＯＭ
４３…ＥＥＰＲＯＭ
４４…信号処理部
４５…ＣＰＵ
４６…データ暗号化エンジン
４７…エラー訂正部
４８…ＵＡＲＴインターフェース
４９…I^2Cインターフェース
５０…リーダ／ライタ機能アナログ回路部

５１…送信アンプ
５２…送信アンテナ
５３…受信信号検出器
５４…受信アンプ・フィルタ
５５…受信アンテナ
１００…データ通信装置

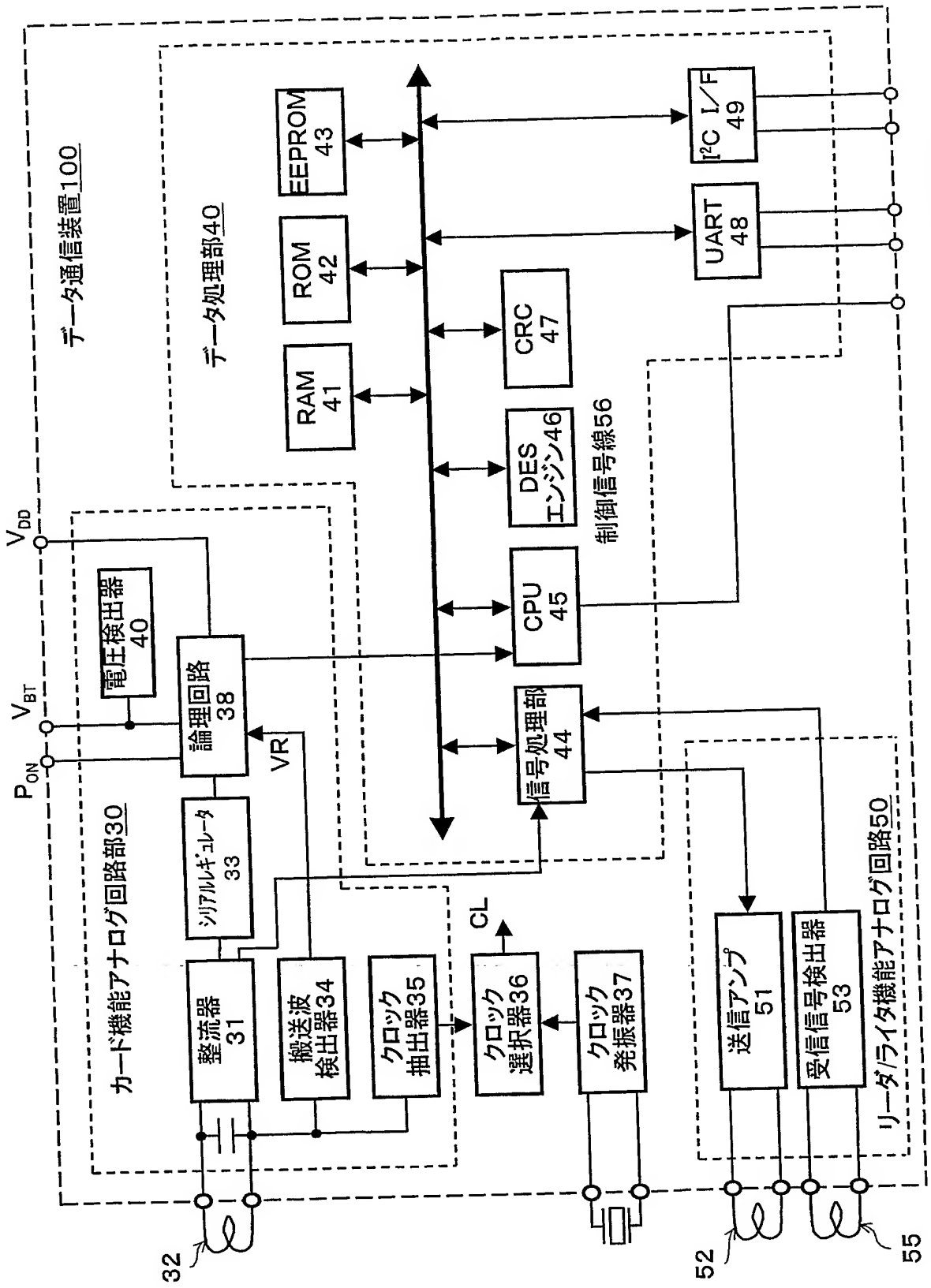
【書類名】図面
【図１】



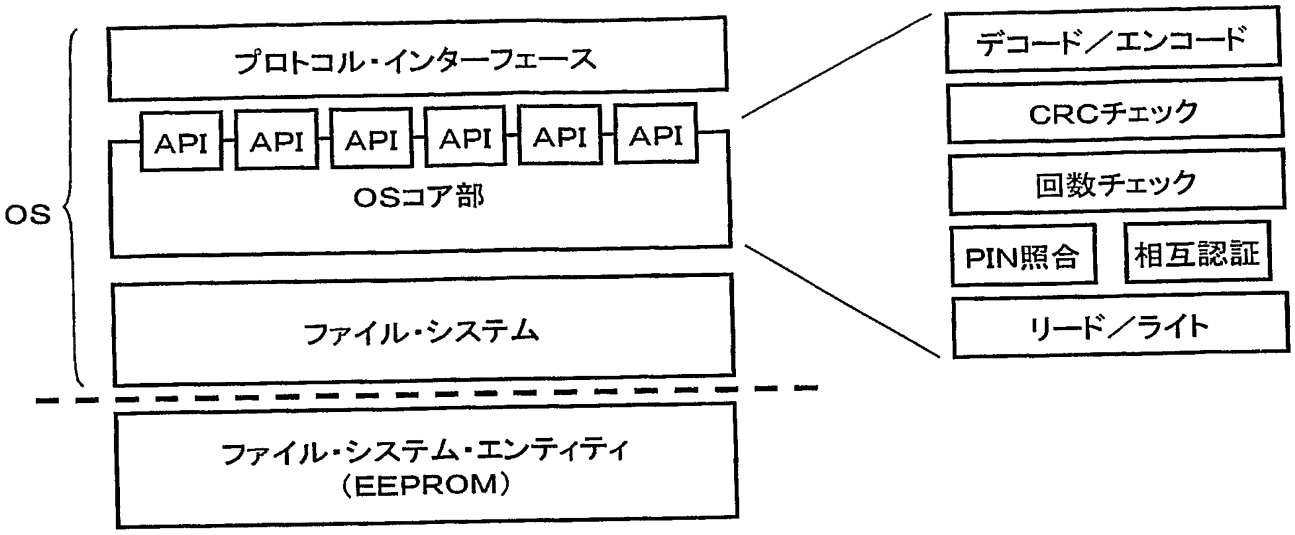
【図２】


ICカード
シーケンサ
メモリ
レギュレータ
復調器
V_2
V_1
Z
変調器
レクティファイヤ
V_o
カード読み書き装置
復調器
プロセッサ
ホストへ

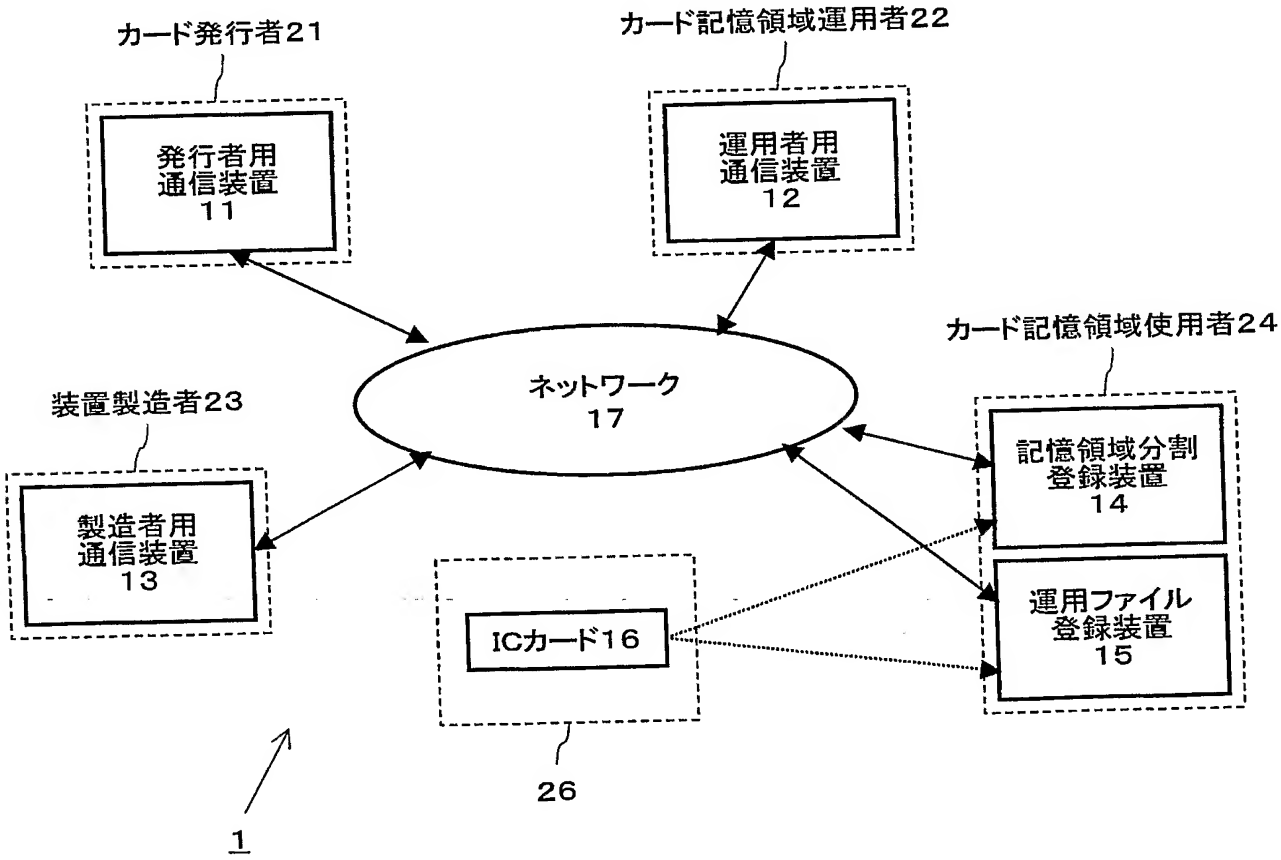
【図３】


データ通信装置100
データ処理部40
カード機能アナログ回路部30
リーダ/ライタ機能アナログ回路50
外部機器へ
制御信号線56
V_{DD}
V_{BT}
P_{ON}
VR
CL
電圧検出器 40
論理回路 38
シリアルI/F 33
整流器 31
搬送波検出器34
クロック抽出器35
クロック選択器36
クロック発振器37
CPU 45
信号処理部 44
DES エンジン46
CRC 47
RAM 41
ROM 42
EEPROM 43
UART 48
I²C I/F 49
送信アンプ 51
受信信号検出器 53
32
52
55

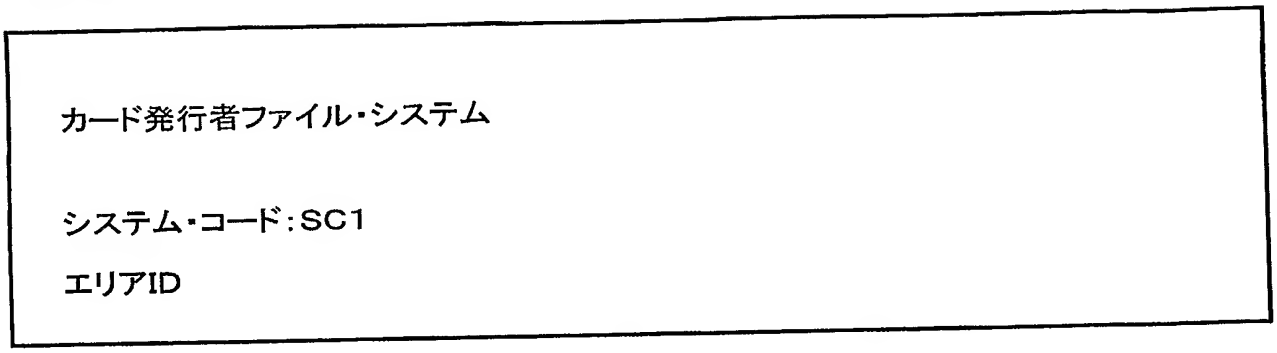
【図４】


プロトコル・インターフェース
API
API
API
API
API
API
OSコア部
OS
ファイル・システム
ファイル・システム・エンティティ
（EEPROM）
デコード／エンコード
CRCチェック
回数チェック
PIN照合
相互認証
リード／ライト

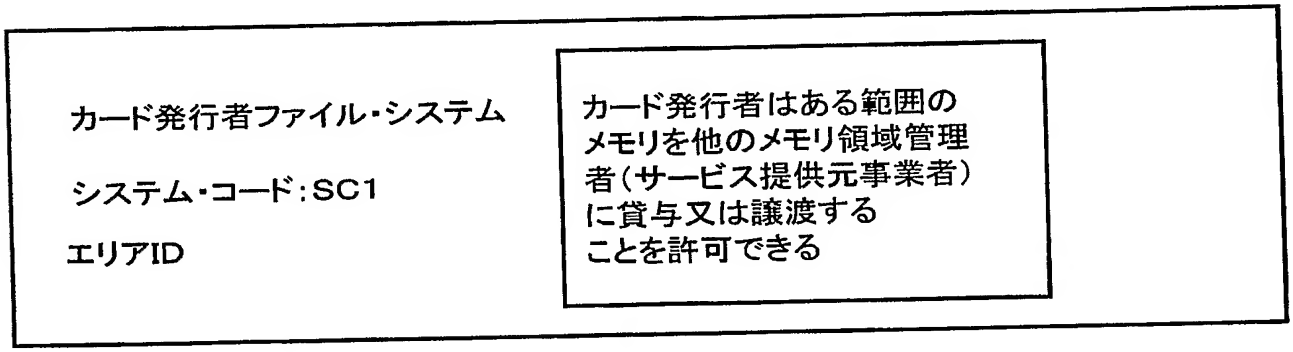
【図５】


カード発行者21
発行者用
通信装置
11
カード記憶領域運用者22
運用者用
通信装置
12
ネットワーク
17
カード記憶領域使用者24
装置製造者23
製造者用
通信装置
13
記憶領域分割
登録装置
14
運用ファイル
登録装置
15
ICカード16
26
1

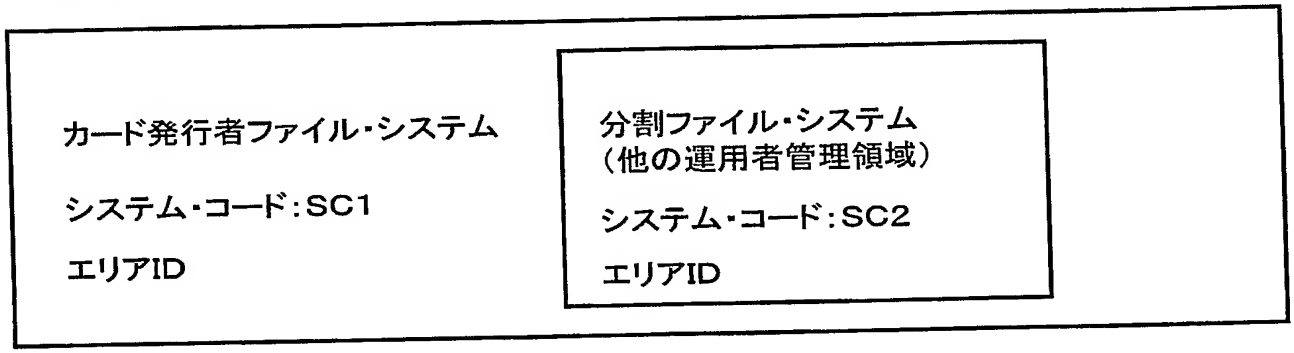
【図６】


カード発行者ファイル・システム
システム・コード：SC1
エリアID

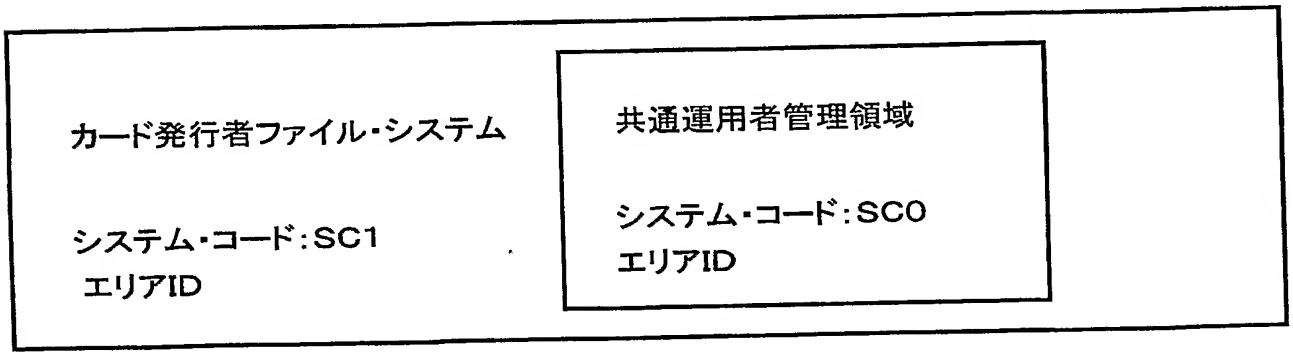
【図７】


カード発行者ファイル・システム
システム・コード：SC1
エリアID
カード発行者はある範囲の
メモリを他のメモリ領域管理
者（サービス提供元事業者）
に貸与又は譲渡する
ことを許可できる

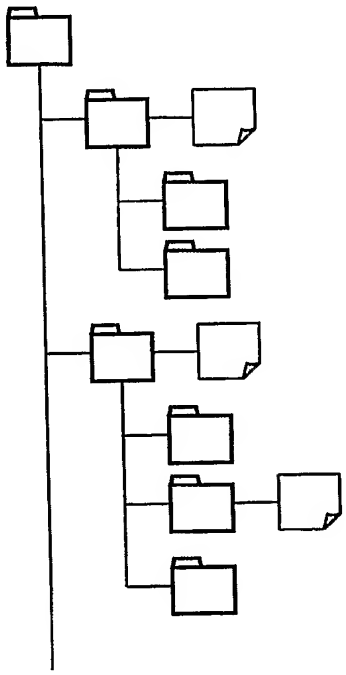
【図８】


カード発行者ファイル・システム
システム・コード：SC1
エリアID
分割ファイル・システム
（他の運用者管理領域）
システム・コード：SC2
エリアID

【図９】

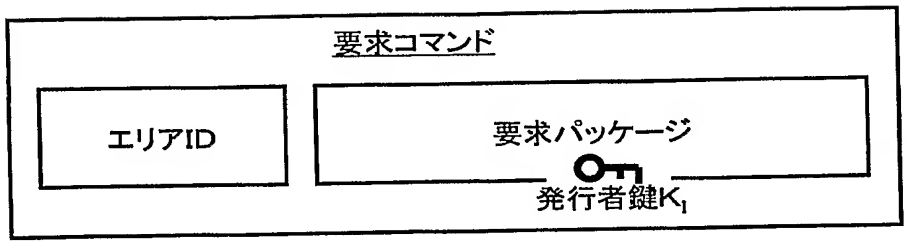

カード発行者ファイル・システム
システム・コード：SC1
エリアID
共通運用者管理領域
システム・コード：SC0
エリアID

【図１０】

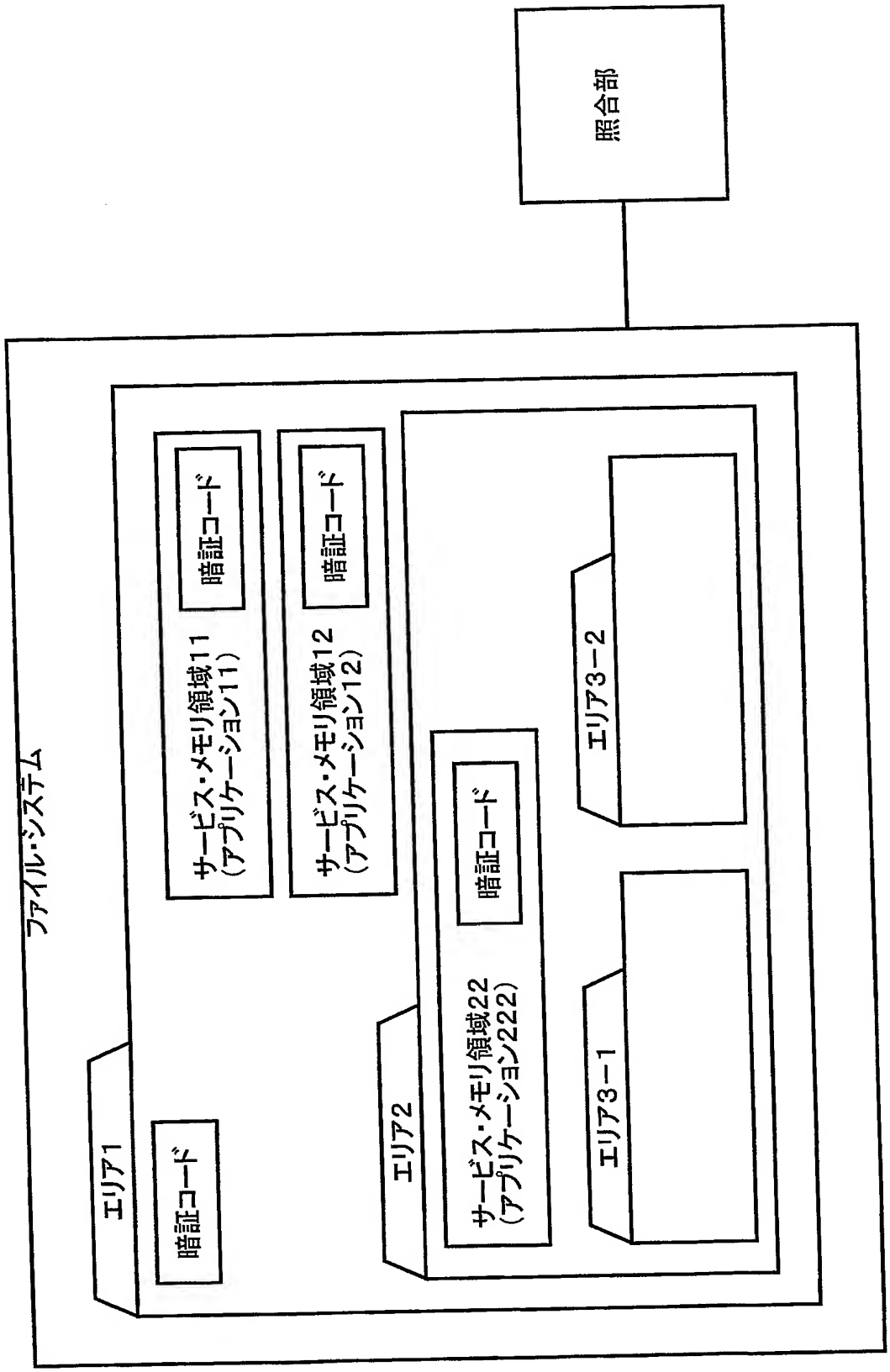
ファイル・システム#0	#1	#1	#1
システム・コードSD#0	SD#1	SD#1	SD#1
エリアID#0	ID#1	ID#1	ID#1
			

.....

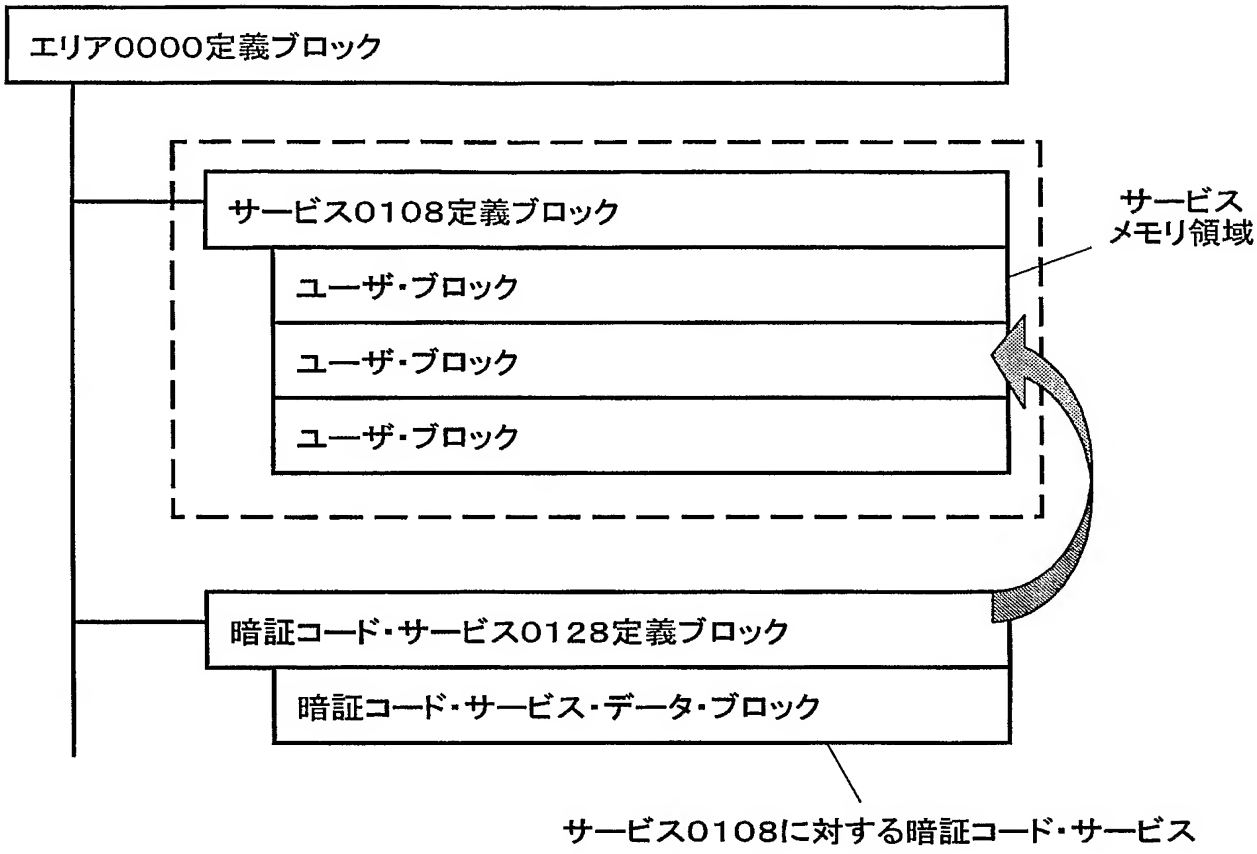
【図１１】



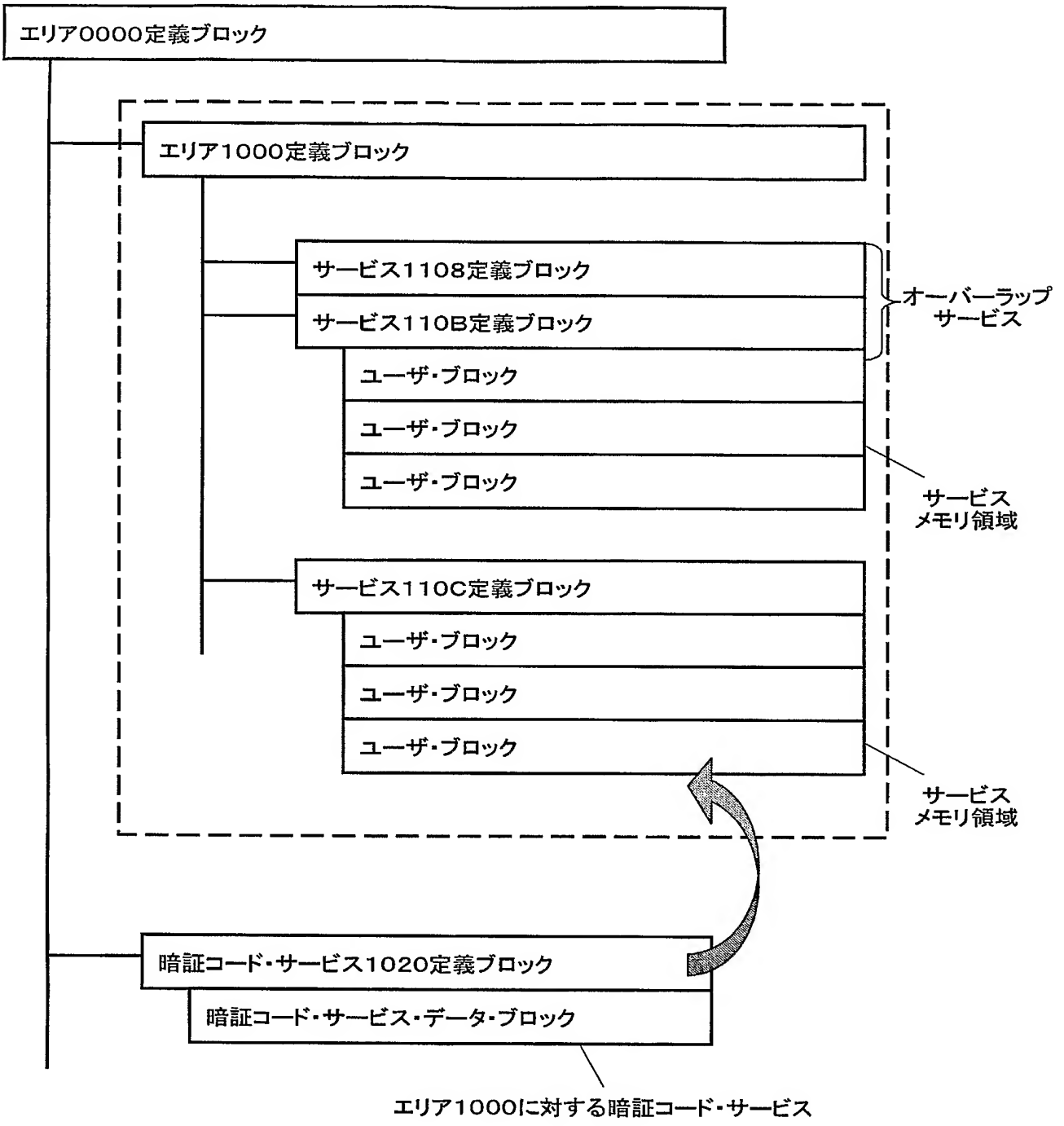
【図１２】


照合部
ファイル・システム
エリア1
暗証コード
サービス・メモリ領域11
(アプリケーション11)
暗証コード
サービス・メモリ領域12
(アプリケーション12)
暗証コード
エリア2
サービス・メモリ領域22
(アプリケーション222)
暗証コード
エリア3－1
エリア3－2

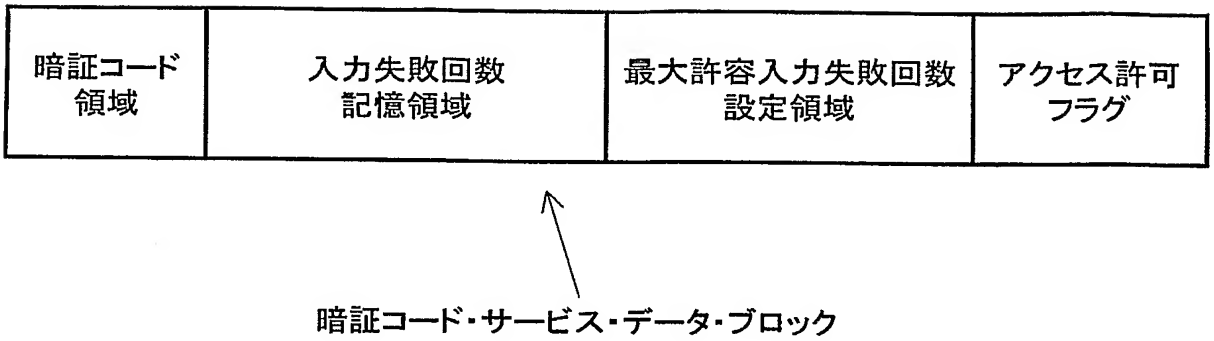
【図１３】


エリア0000定義ブロック
サービス0108定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
暗証コード・サービス0128定義ブロック
暗証コード・サービス・データ・ブロック
サービス0108に対する暗証コード・サービス

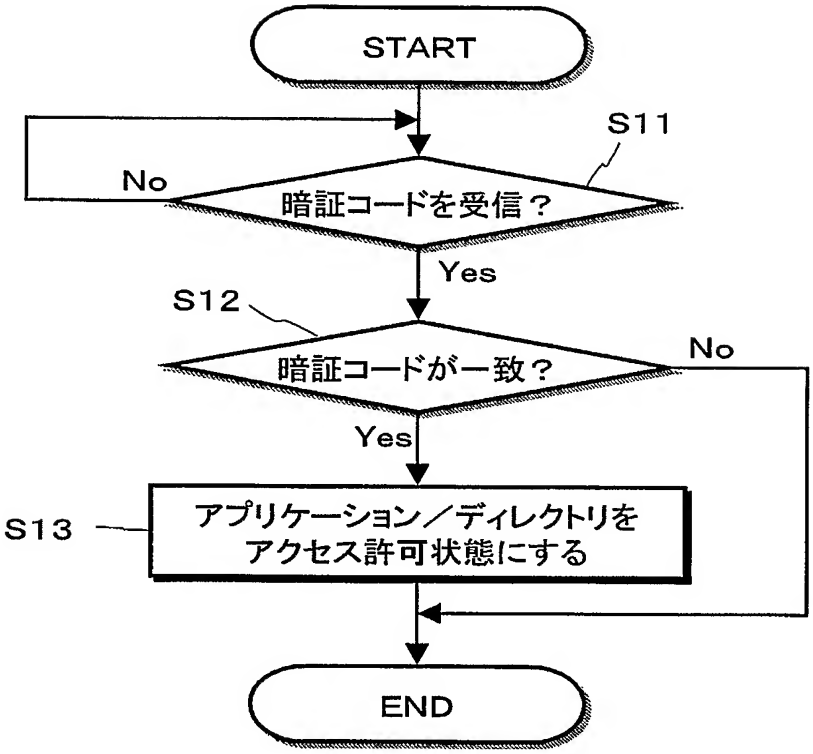
【図１４】


エリア0000定義ブロック
エリア1000定義ブロック
サービス1108定義ブロック
サービス110B定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
オーバーラップ
サービス
サービス
メモリ領域
サービス110C定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
暗証コード・サービス1020定義ブロック
暗証コード・サービス・データ・ブロック
エリア1000に対する暗証コード・サービス

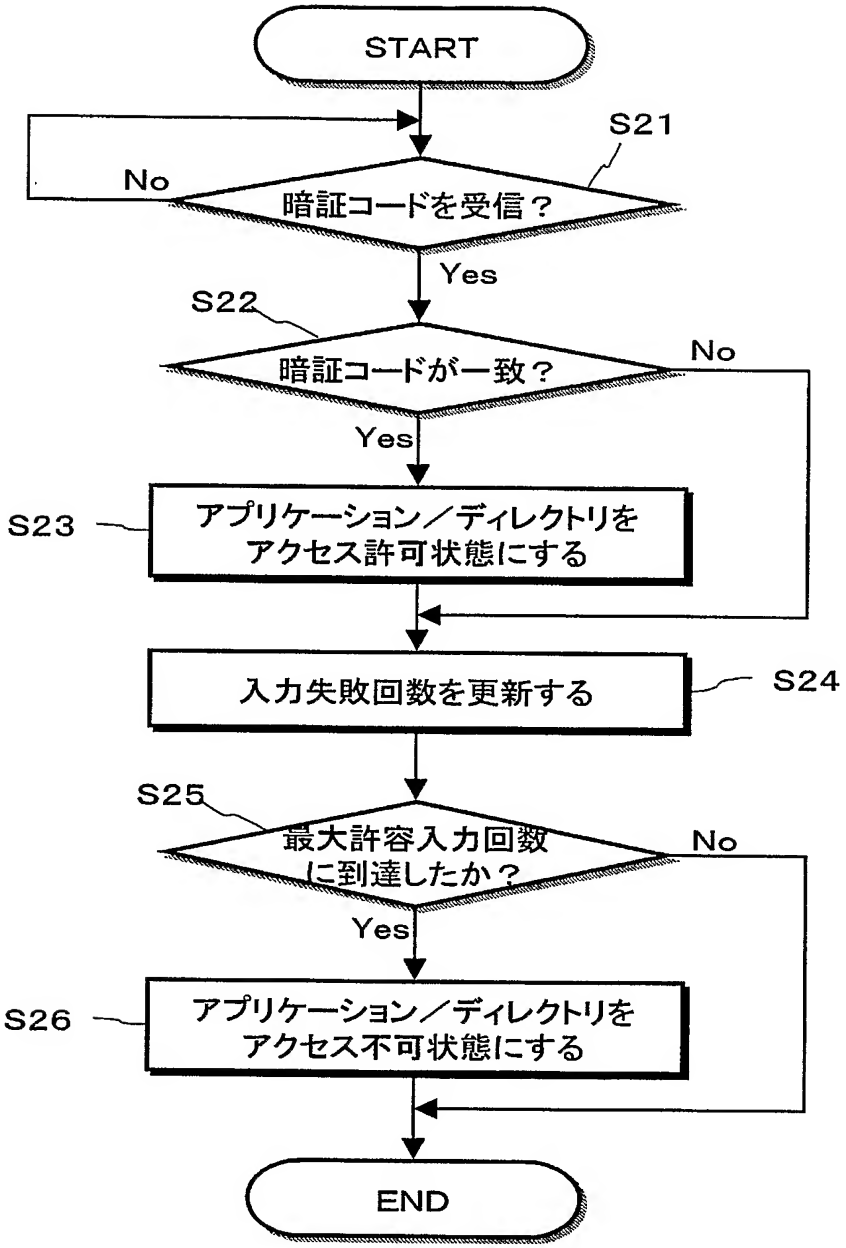
【図１５】


暗証コード
領域
入力失敗回数
記憶領域
最大許容入力失敗回数
設定領域
アクセス許可
フラグ
暗証コード・サービス・データ・ブロック

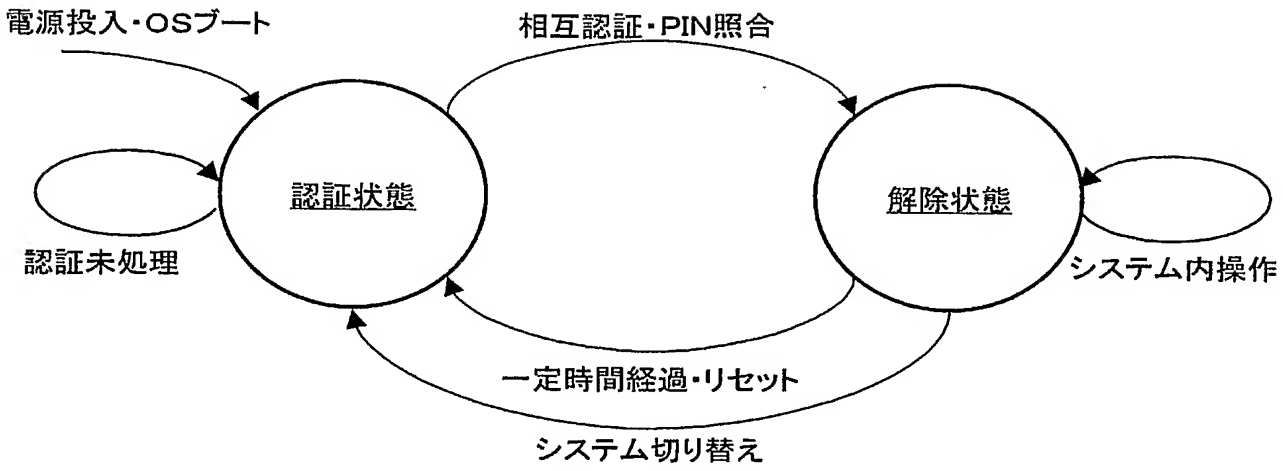
【図１６】


START
S11
No
暗証コードを受信？
Yes
S12
暗証コードが一致？
No
Yes
S13
アプリケーション／ディレクトリを
アクセス許可状態にする
END

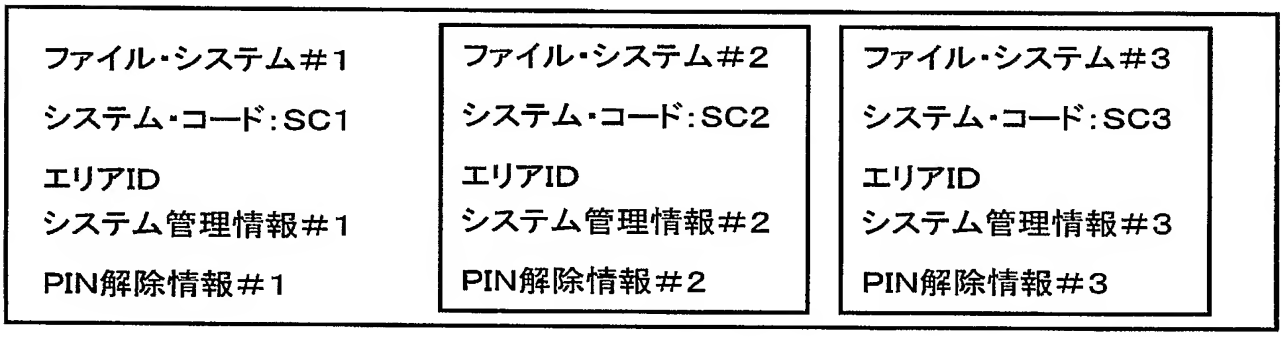
【図１７】


START
S21
No
暗証コードを受信？
Yes
S22
暗証コードが一致？
No
Yes
S23
アプリケーション／ディレクトリを
アクセス許可状態にする
入力失敗回数を更新する
S24
S25
最大許容入力回数
に到達したか？
No
Yes
S26
アプリケーション／ディレクトリを
アクセス不可状態にする
END

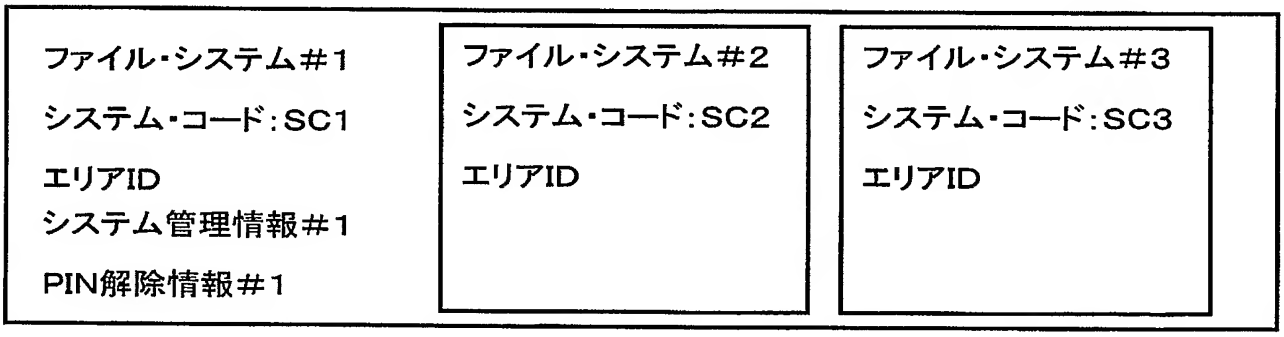
【図１８】



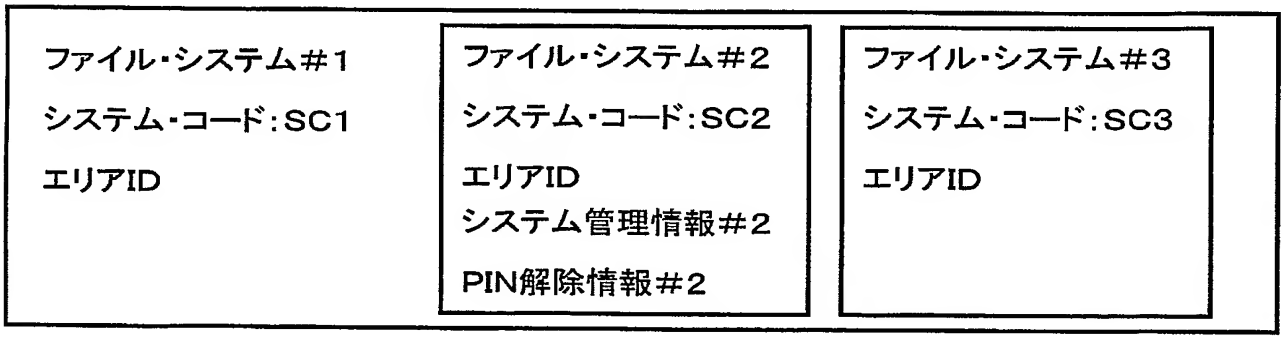
【図１９】



【図２０】



【図２１】



【書類名】要約書
【要約】
【課題】　メモリ領域上の事業者毎の情報をセキュアに管理する機構を備え、単一のＩＣカードを複数のサービス提供元事業者間で共用する。
【解決手段】　単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一の情報記憶媒体を複数の事業者で共有する。メモリ領域をファイル・システムに分割する。ファイル・システム間の境界がファイヤ・ウォールとして機能し、不正侵入を好適に排除する。さらに、ファイル・システムの分割機能と、各ファイル・システムに対する暗証コードの照合機能を連携させ、ファイル・システム毎に独立してセキュリティ管理を実現する。
【選択図】　図１８

特願２００４－００１３５９

出　願　人　履　歴　情　報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社